ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

“ELABORAR EL PLAN DE CONTINGENCIA INFORMÁTICO, DE LA UNIDAD DE NEGOCIO HIDROPAUTE CELEC EP, QUE PERMITA GARANTIZAR LA CONTINUIDAD DE LAS ACTIVIDADES ANTE EVENTOS QUE PODRÍAN ALTERAR EL NORMAL FUNCIONAMIENTO DE LA TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN (TIC).**”**

TESIS DE GRADO

Previa la obtención del Título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Presentada por:

Alfredo Marcelo Carpio Cobos

Guayaquil – Ecuador

Año 2015

AGRADECIMIENTO

A Dios, y a todas las personas, compañeros, amigos y colegas que permitieron con su ayuda y apoyo culminar este trabajo y meta profesional.

DEDICATORIA

A mis hijos y esposa por su apoyo y comprensión en todo este tiempo que ha tomado mi preparación profesional, han sido mi soporte incondicional en todo momento.

TRIBUNAL DE SUSTENTACIÓN

Mgs. Lenin Freire C.
Director MSIA

Mgs. Albert Espinal S.
Director de Tesis

Mgs. Robert Andrade T.
Miembro Principal

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponden exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL"

Alfredo Marcelo Carpio Cobos

RESUMEN

El presente trabajo tuvo como fin la posibilidad de establecer un plan de contingencia informático dentro de una de las empresas publicas estratégicas del Ecuador que aporta con alrededor del 32% de promedio de energía eléctrica al país, teniendo como alcance la Central Hidroeléctrica Paute-Mazar que entro a operar comercialmente en el año 2010.

Para el efecto se han tomado como base algunas de las buenas prácticas y normativas nacionales e internacionales existentes en el mercado como: ITIL, COBIT, MAGERIT, NTE INEN-ISO/IEC 27002, FAMILIA ISO 27000 , NIST 800-34; las mismas que han permitido realizar un adecuado análisis y elaboración de un plan de contingencia informático que permita a la Unidad de Negocio Hidropaute y en especial al Área de TIC estar preparada ante un evento que cause la falta de entrega de sus recursos tecnológicos comprometidos para poder producir de manera adecuada su producto o servicio final a sus clientes.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

CCAD	Estación de Ingeniería
CCC	Centralog Configuration Center
CIS	Centralog Interfaz System
CPCI	Coordinador del Plan de Contingencias Informático
C10	Estación de Operación Centralog
ETC	Etcétera
ICCP	Inter-Control Center Communications Protocol
ING	Ingeniero
ISO	Organización Internacional de Normalización
ISP	Internet Service Provider
ITIL	Biblioteca de Infraestructura de Tecnologías de la Información
OPMZ	Operación Mazar
RCMZ	Redes y Comunicaciones Mazar
SCADA	Supervisión, Control y Adquisición de Datos
SPMZ	Soluciones de Producción Mazar

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Uno de los aspectos fundamentales y que han venido predominando con el pasar de los tiempos y que se presenta en el entorno tanto educativo, familiar, industrial, etc., es el uso de la tecnología como herramienta importante de sustento para el convivir diario y entrega de productos o servicios asociados a su razón de ser, en especial en el ámbito industrial y rama eléctrica se han venido notando cambios importantes tanto así que se depende de estos elementos tecnológicos cada vez más , en este aspecto centrales hidroeléctricas como Paute-Mazar no se han quedado atrás y en la actualidad dependen en un gran porcentaje de estas tecnologías para entregar su producto a sus potenciales clientes.

La Unidad de Negocio Hidropaute (Central Paute-Mazar) requiere contar con un Plan de Contingencia Informático, que le permita estar preparada ante un desastre, es decir a la interrupción prolongada de los servicios informáticos y teniendo en cuenta que se encuentra regulada por la Contraloría General del Estado la cual emitió el Acuerdo 039-CG de 16 de noviembre del 2009, suscrito por el doctor Carlos Pólit Faggioni, Contralor General del Estado, mediante el cual expide las “Normas de Control Interno para las entidades,

organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos", misma que es publicada en el Registro Oficial (01-12-2009) con el N° 78 y Suplemento Registro Oficial (14-12-2009) N° 87 (Anexo A), el cual hace referencia en su numeral 410-11 "Corresponde a la Unidad de Tecnología de Información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado."

Para concretar el objetivo se ha realizado un análisis del contexto de la organización, se establece un plan de contingencias, donde se define su alcance, ámbito, compromisos y responsabilidades respectivas, se genera un análisis de Impacto en el negocio junto con la metodología MAGERIT se procede a elaborar un análisis de riesgos y se determinan estrategias para establecer e implementar procedimientos de contingencia.

CAPÍTULO 1

INTRODUCCIÓN AL PLAN DE CONTINGENCIA.

1.1 Conceptos básicos de Plan de Contingencia

¿Qué es un Plan de Contingencia?

Hoy en día sin temor a equivocarse, se podría decir que una organización basa su operatividad, así como la consecución de sus objetivos, en un porcentaje alto en el correcto funcionamiento de sus equipos informáticos.

No cabe duda que cualquier daño ocasionado a los sistemas informáticos podría desencadenar en interrupciones o paralizaciones de mayor o menor grado comprometiendo la continuidad de las operaciones, ocasionando consecuencias

negativas, especialmente de índole económico a las organizaciones.

Una manera de poder contrarrestar estas consecuencias negativas se basa en la creación de un Plan de Contingencia, pudiendo definirlo como “El conjunto de procedimientos de tipo preventivo, cuya misión es aportar la infraestructura necesaria para la puesta en marcha de una recuperación del sistema, en caso de producirse un desastre” [1] o un evento, incidente o situación que pueda paralizar, ya sea de forma parcial o total los servicios de la organización, enfocados a recuperar los mismos de manera ágil y dinámica, de tal manera de seguir operando aunque sea a un nivel mínimo aceptable.

Entendiéndose por Recuperación, "tanto la capacidad de seguir trabajando en un plazo mínimo después de que se haya producido el problema, como la posibilidad de volver a la situación anterior al mismo, habiendo reemplazado o recuperado el máximo posible de los recursos e información" [2].

Tipos de contingencia

Se pueden establecer diferentes tipos de contingencia basados en los daños sufridos y grado de afectación.

De acuerdo a los daños sufridos:

1. Menor.- Afecta sólo la operación diaria y siendo su tiempo de recuperación menor a 8 horas [3].
2. Grave.- Produce daños a las instalaciones, pudiendo reiniciar las operaciones en menos de 24 horas [3].
3. Crítica.- Afecta tanto la operación y las instalaciones, no es factible su recuperación en corto tiempo, debido a falta de normas preventivas o insuficientes, también podría suceder por un desastre natural como terremoto, inundaciones, etc., [3].

De acuerdo al grado de afectación [3]:

1. En el mobiliario.
2. Instalaciones.
3. Hardware.
4. Software y utilitarios.

5. Datos e Información.
6. Documentación.
7. Comunicaciones (hubs, ruteadores, nodos, telefonía).

1.2 Objetivos del Plan de Contingencia

Podremos enumerar los siguientes:

1. Proveer una solución para mantener operativos los servicios críticos que componen los Sistemas de Información, los cuales son fundamentales para la organización, cuando estos son paralizados parcial o totalmente.
2. Establecer de manera clara y concisa todas las acciones y procedimientos a realizar en el caso que se presenten incidentes, fallos o daños sobre los elementos que componen el Sistema de Información.

1.3 Seguridad integral de la información

Las organizaciones actuales están conscientes que el valor más importante radica en los datos e información registrados en sus sistemas informáticos, así como del soporte adecuado de las TIC para facilitar su almacenamiento, procesamiento, análisis y distribución, dejando de lado a los elementos productivos los cuales

eran la base efectiva del negocio, hoy en día más importante que la máquina misma es la información que permite saber qué, cómo y cuándo hacer algo, en consecuencia se torna imprescindible proteger a las organizaciones de una fuga incontrolada de información.

Ante esto es necesario aplicar medidas de seguridad que estén basadas en la definición de controles físicos (que afecta a la infraestructura y los recursos informáticos) y lógicos (para proteger datos, aplicaciones y sistemas operativos).

En relación a la seguridad misma de la información, estas medidas han de tenerse en cuenta para obtener una adecuada Confidencialidad, Integridad, Disponibilidad (Figura 1.1), “desde un punto de vista más amplio, en la norma ISO/IEC 17799 se define la Seguridad de la Información como la preservación de su confidencialidad, su integridad y su disponibilidad” [4].

La norma ISO/IEC 27001:2013 nos dice que “El sistema de gestión de seguridad de la información preserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación

de un proceso de gestión de riesgos y da confianza a las partes interesadas de que los riesgos se gestionan adecuadamente.”

Figura 1.1.Seguridad de la Información según la norma ISO/IEC 17799.

Fuente: (Vieites, 2011, pág. 39)

Elaborado por: Alfredo Carpio

Confidencialidad

Garantiza que cada mensaje transmitido o almacenado en un sistema informático sólo podrá ser leído por la persona o sistema que esté autorizado.

Una persona o sistema no autorizado no podrá acceder al contenido del mensaje original, garantizando de esta manera la confidencialidad de los datos almacenados en un equipo, de los datos guardados en dispositivos de respaldo y/o de los datos transmitidos a través de redes de comunicaciones.

Integridad

Cualidad que tiene un mensaje, documento o fichero que no ha sido modificado desde su creación o durante su transmisión a través de una red informática, pudiendo así detectar alguna modificación de algún dato en un mensaje, documento o fichero almacenado, procesado o transmitido por un sistema o red informática.

Disponibilidad

Se refiere a la continuidad operativa de la organización, asegurando que la información y los sistemas que la soportan (estructura física y tecnológica que permite el acceso, tránsito y almacenamiento de la información), estén disponibles en el momento en que se necesiten, para los usuarios autorizados a utilizarlos.

Debiendo también considerar la recuperación del sistema frente a posibles incidentes de seguridad que se presenten, sin dejar de lado a desastres naturales o intencionados (incendios, inundaciones, sabotajes, etc.) que provocarían indisponibilidad de los servicios, datos o sistemas.

1.4 Gestión de riesgos de Seguridad de la Información

Riesgo

"El riesgo es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad y se convierta en un desastre, causando un determinado impacto en la organización" [4].

La vulnerabilidad o las amenazas, por separado, no representan un peligro, pero si se juntan, se convierten en un riesgo, es decir, en la probabilidad de que ocurra un desastre.

Según la Norma ISO 27005:2008 un riesgo de seguridad de la información es "una potencial amenaza que explota las vulnerabilidades de un activo o grupo de activos y por lo tanto causan daño a la organización".

El logro de los objetivos organizacionales depende de factores internos y externos, que introducen un nivel de incertidumbre que la organización tiene que enfrentar. El efecto que esta incertidumbre tiene en los objetivos de la organización se denomina riesgo, de acuerdo a la norma ISO 31000:2009 ISO Guide 73 dice que “el riesgo es el efecto de la incertidumbre en los objetivos”.

Existen algunas metodologías de gestión de riesgos como:

1. MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas), país España.
2. CRAMM (CCTA Risk Analysis and Management Method), país Reino Unido.
3. MARION (propuesta en 1985 por la Asociación de Empresas Aseguradoras Francesas).
4. MELISA (definida en 1984 dentro del entorno militar francés).
5. EBIOS (DCSSI - Francia).

6. IT Baseline Protection Manual (BSI - Alemania).

7. NIST SP800-30 (NIST – Estados Unidos).

Hay varias herramientas, como Pilar y Cramm, que implícitamente aplican algunas de estas metodologías y ayudan al proceso de evaluación de riesgos, además ofrecen características tales como bases de conocimiento, flujos de trabajo, así como el cálculo automático.

Vulnerabilidad

Es cualquier debilidad en el sistema informático que pueda permitir a las amenazas causarle daños producir pérdidas en la organización.

Las vulnerabilidades se corresponden con fallos en los sistemas físicos y/o lógicos, aunque también pueden tener su origen en los defectos de ubicación, instalación, configuración y mantenimiento de los equipos.

Pueden estar ligadas a aspectos organizativos (procedimientos mal definidos o sin actualizar, ausencia de políticas de seguridad ...), al factor humano (falta de formación y/o de sensibilización del personal con acceso a los recursos del sistema), a los propios equipos, a los programas y herramientas lógicas del sistema, a los locales y las condiciones ambientales del sistema (deficientes medidas de seguridad físicas, escasa protección contra incendios, mala ubicación de los locales con recursos críticos para el sistema, etc.).

Se suele emplear una escala cuantitativa o cualitativa para definir el nivel de vulnerabilidad de un determinado equipo o recurso: Baja, Media y Alta.

Amenaza

Algún tipo de mecanismo que al activarse causa un incidente no deseado, provocando un daño a un sistema u organización.

Incidente de Seguridad

Un incidente de seguridad es cualquier evento que tenga o pueda tener como resultado la interrupción de los servicios suministrados

per un sistema informático y/o posibles pérdidas físicas, de activos o financieras. Es decir, se considera que un incidente es la materialización de una amenaza.

Impacto

El impacto es la medición y valoración del daño que podría producir a la organización un incidente de seguridad, generando cambios adversos en los objetivos de la organización.

Para valorar el impacto es necesario tener en cuenta tanto los daños tangibles como la estimación de los daños intangibles (incluida la información). En este sentido, podría resultar de gran ayuda la realización de entrevistas en profundidad con los responsables de cada departamento, función o proceso de negocio, tratando de determinar cuál es el impacto real de la revelación, alteración o pérdida de la información para la organización, y no sólo del elemento TIC que la soporta.

También en este caso se puede emplear una escala cuantitativa o cualitativa para medir el impacto del daño en la organización: Bajo, Moderado y Alto.

Gestión del Riesgo

Un proceso de gestión de riesgos comprende una etapa de evaluación previa de los riesgos del sistema informático, que se debe realizar con rigor y objetividad para que cumpla su función con garantías. Para ello, el equipo responsable de la evaluación debe contar con un nivel adecuado de formación y experiencia previa, así como disponer de una serie de recursos y medios para poder realizar su trabajo, contando en la medida de lo posible con el apoyo y compromiso de la Alta Dirección.

En el proceso propiamente dicho de gestión de riesgos se trata de definir un plan para la implantación de ciertas salvaguardas o contramedidas en el sistema informático, que permitan disminuir la probabilidad de que se materialice una amenaza, o bien reducir la vulnerabilidad del sistema o el posible impacto en la organización, así como permitir la recuperación del sistema o la transferencia del problema a un tercero (Figura 1.2).

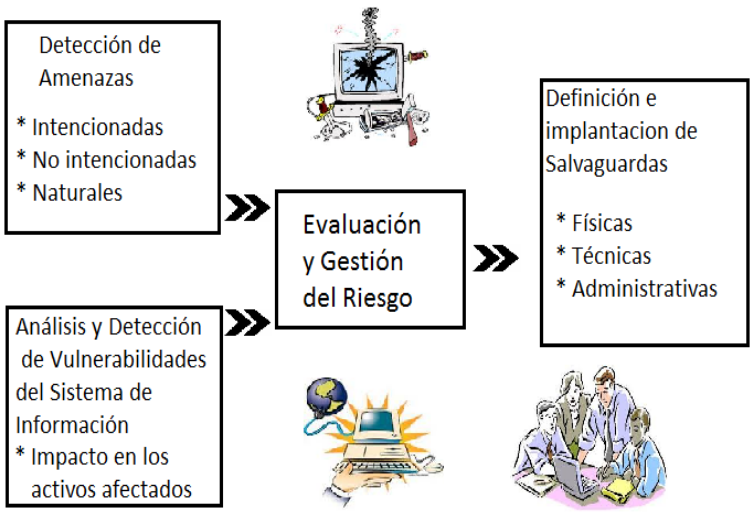


Figura 1.2. Análisis y Gestión de Riesgos en una Organización.

Fuente: (Vieites, 2011, pág. 59)

Elaborado por: Alfredo Carpio

Cuando no se implementa un plan de riesgos, la organización carece de un soporte para el contexto estratégico de la organización, para sus metas, objetivos y la naturaleza de su negocio, no se aseguraría el correcto funcionamiento en todos los niveles de la organización.

1.5 Familia ISO/IEC 27000, COBIT, ITIL y NIST SP 800-34

ISO/IEC 27000

La ISO/IEC 27000 es una serie de estándares enfocados con los Sistemas de Gestión de Seguridad de la Información (SGSI), los rangos de numeración van de 27000 a 27019 y de 27030 a 27044. Las definiciones relevantes que antes se encontraban en la ISO 27001 fueron movidas a ISO27000.

ISO/IEC 27001

Su última versión con cambios tanto en su contenido y estructura es la ISO/IEC 27001:2013 fue publicada el 25 de Septiembre 2013, la cual ayuda a las organizaciones a gestionar la seguridad de la información, permitiendo adaptarse a la nueva estructura de alto nivel utilizado en todas las normas de Sistemas de Gestión, desarrollada en base al Anexo SL (Figura 1.3) de ISO/IEC (anteriormente publicado como Guía ISO:83), lo cual impedirá problemas de integración con los diversos marcos de referencia existentes y nuevas, cabe recalcar que esta norma es certificable.

Figura 1.3. Estructura ISO/IEC 27001:2013 basada en el Anexo SL

Fuente: Norma ISO/IEC 27001:2013

Elaborado por: Alfredo Carpio

El Anexo A - Referencia de objetivos y controles que forma parte de este estándar, tiene las siguientes características:

1. Dominios: 14
2. Controles:114

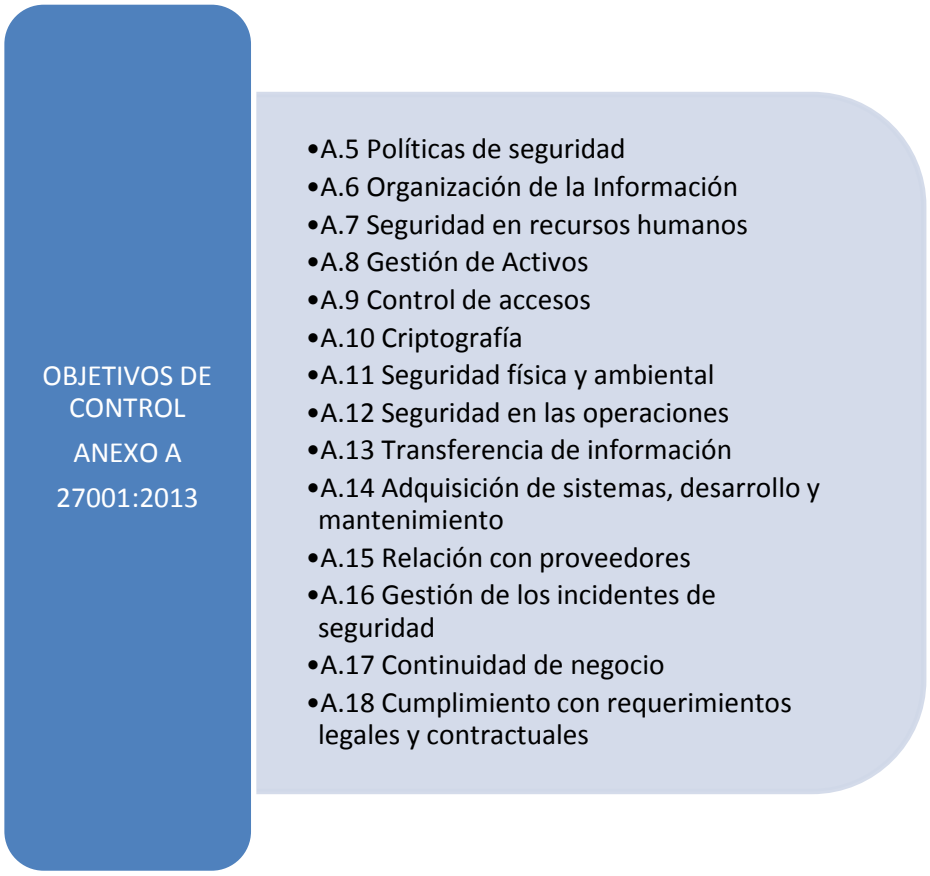


Figura 1.4. Dominios de ANEXO A 27001:2013

Fuente: Norma ISO/IEC 27001:2013

Elaborado por: Alfredo Carpio

ISO/IEC 27002

Su última versión ISO/IEC 27002:2013 fue publicada junto con la norma 27001 en Octubre del año 2013, es una guía de buenas prácticas para la seguridad de la información**.**

La norma se refiere explícitamente a la información de seguridad, es decir, la seguridad de todas las formas de información (por ejemplo, los datos informáticos, documentación, conocimiento y propiedad intelectual) y no sólo seguridad de los sistemas TIC o "ciberseguridad" este último de moda o actualidad.

Describe 35 objetivos de control (uno por cada categoría de control de seguridad) y 114 controles recomendables en cuanto a seguridad de la Información, que se agrupan en 14 dominios (Figura 1.4). La norma ISO/lEC 27001 contiene un Anexo A que resume todos los controles de la ISO/lEC 27002. Esta norma no es certificable.

ISO/IEC 27005

Esta norma fue publicada en segunda edición el 1 de Junio del 2011 a modo de guía, con una serie de directrices basada en un

enfoque de gestión de riesgos en la seguridad de la información y que apoya de manera particular los requisitos del sistema de gestión de seguridad de la información definidos en la ISO 27001.

En Ecuador la norma que hace referencia a la ISO/IEC 27005 la cual se ha editado y adaptado a nuestro ámbito es la Norma Técnica Ecuatoriana NTEISO/IEC 27005.

Esta norma no es ni recomienda una metodología concreta (en el punto 1.5 se listaron algunas metodologías de tratamiento del riesgo) deja libertad a las organizaciones en seleccionar la metodología que se ajuste a sus diferentes necesidades, más bien es una descripción de “qué hacer” para llevar a cabo un proceso de gestión de riesgos, en un dominio específico de seguridad de la información, No explica el “Cómo hacer” y no es certificable, lo conforman las siguientes fases (Figura 1.5):

1. Establecimiento del contexto (Cláusula 7)
2. Evaluación del riesgo (Cláusula 8)
3. Tratamiento del riesgo (Cláusula 9)
4. Aceptación del riesgo (Cláusula 10)

5. Comunicación del riesgo (Cláusula 11)
6. Monitorización y revisión del riesgo (Cláusula 12)

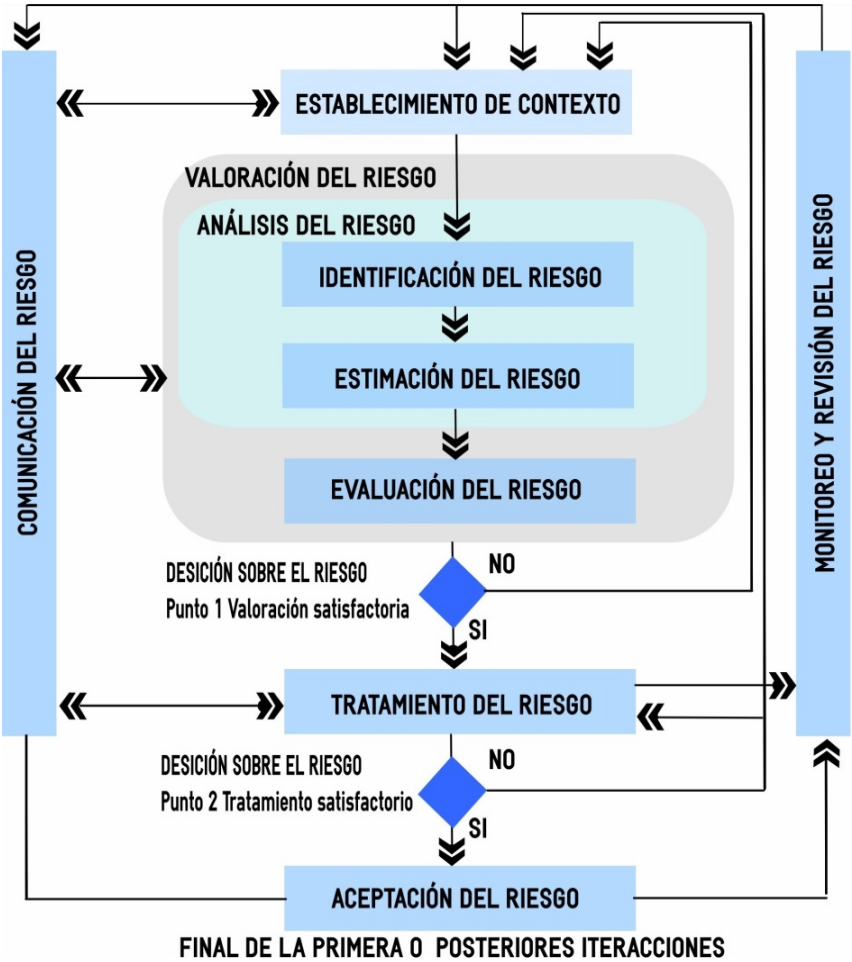


Figura 1.5. Proceso gestión del riesgo seguridad de la información 27005

Fuente: Norma NTISO/IEC Ecuatoriana 27005

Elaborado por: Alfredo Carpio

COBIT

ISACA (Information Systems Audit and Control Association), fundada en 1969 creo el IT Governance Institute (ITGI) para promover el pensamiento internacional sobre cuestiones actuales y futuras relativas a la administración, seguridad y aseguramiento de Tecnologías de la Información.

Es así que entre sus documentos tienen uno que a nivel mundial es sumamente reconocido, es COBIT (Objetivos de control para tecnologías de la información y similares).

COBIT es un marco de referencia de negocios compatible con ISO/IEC 27002 y COSO (Committee of Sponsoring Organizations), donde se incorpora aspectos fundamentales de otros estándares relacionados; es decir todas aquellas empresas que estén utilizando las prácticas señaladas por COBIT están más cerca de adaptarse y lograr de así requerirlo la certificación en ISO 27001.

Actualmente COBIT 5 es el marco de gestión y de negocio integral donde se establecen principios, prácticas, herramientas y modelos de análisis mundialmente aceptados que ayuda a las

organizaciones a lograr su metas y entregar valor mediante el gobierno y la gestión de las TI, tiene 5 principios (Figura 1.6) y define 7 catalizadores/habilitadores (Figura 1.7) genéricos que componen el marco, lo que permite que sean útiles para las organizaciones de cualquier tamaño, de carácter comercial, sin fines de lucro o en el sector público.

Figura 1.6. Los principios de COBIT 5

Fuente: COBIT 5, Introduction Spanish 2012 ISACA

Elaborado por: Alfredo Carpio

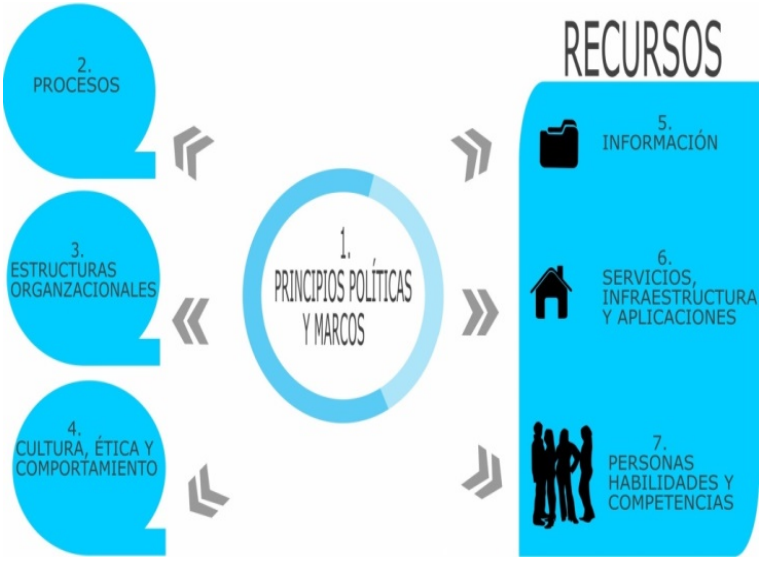


Figura 1.7. Habilitadores de COBIT 5

Fuente: COBIT® 5, Introduction Spanish © 2012 ISACA®

Elaborado por: Alfredo Carpio

No existe una certificación en las prácticas indicadas por COBIT, más bien ISACA ofrece certificaciones personales a profesionales tales como:

1. CISA (Certified Information Systems Auditor).
2. CISM (Certified Information Security Manager).
3. CGEIT (Certified in the Governance of Enterprise IT).
4. CRISC (Certified in Risk and Information Systems Control).

ITIL

Information Technology Infrastructure Library (Biblioteca de Infraestructura de Tecnologías de Información), fue desarrollada en el año 1980, es un marco de referencia donde se establece un conjunto de mejores prácticas y recomendaciones para la administración de servicios de TI, con un enfoque de administración de procesos.

Tomo auge a mediados de los años 1990, en 2007 se libera de la versión 3 de ITIL y en el verano del 2011 se libera edición 2011.

ITIL 2011 Edition consta de cinco libros:

1. Estrategia de servicios.
2. Diseño de servicios.
3. Transición de servicios.
4. Operación de servicios.
5. Mejora continua de servicios.

Todas actividades referentes a la administración de la seguridad están inmersas en casi todos los procesos de ITIL, debido a que es

de vital importancia dentro de una adecuada administración, identificar los riesgos asociados al proceso para definir líneas de acción, con la finalidad de mitigarlos; por lo anterior, cobra especial relevancia el tópico "Security Management" que forma parte de la biblioteca.

NIST SP 800-34

La publicación especial 800-34 Planes de Contingencia Guía de Ayuda para los Sistemas de Información del National Institute for Standards and Technology (NIST, o Instituto Nacional de Estándares y Tecnología) de los Estados Unidos, proporciona las instrucciones, recomendaciones y consideraciones para la planificación de contingencia de la información del sistema. La planificación de contingencia se refiere a las medidas necesarias para recuperar los servicios de información del sistema después de una interrupción. Estas medidas provisionales pueden incluir la reubicación de los sistemas de información y operaciones a un lugar alternativo, la recuperación de las funciones de sistema de información utilizando un equipo alternativo, o el desempeño de las funciones de sistema de información utilizando métodos manuales. Además da las recomendaciones específicas de planificación de

contingencia para tres tipos de plataforma y proporciona estrategias y técnicas comunes a todos los sistemas [5].

1. Los sistemas cliente / servidor.
2. Sistemas de telecomunicaciones.
3. Sistemas mainframe (Unidad Central).

La estructura del plan de contingencia de acuerdo a la NIST 800-34 deberá tener 7 pasos fundamentales como se ve en la Figura 1.8.

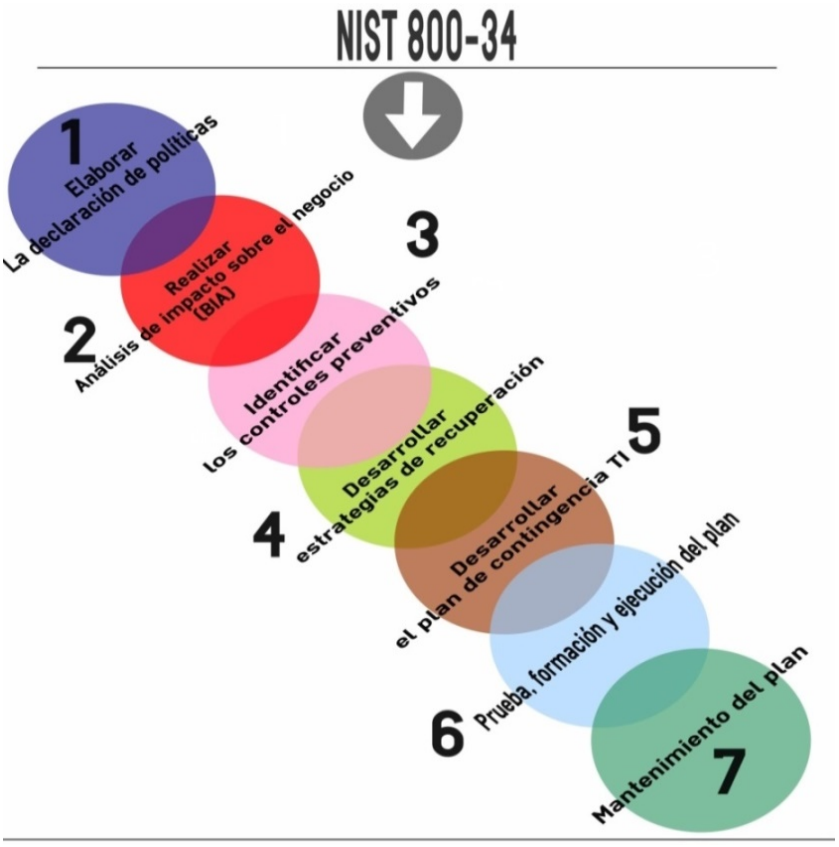


Figura 1.8. Estructura Plan de Contingencia

Fuente: (NIST National Institute of Standards and Technology, 2010)

Elaborado por: Alfredo Carpio

CAPÍTULO 2

ANÁLISIS DE RIESGO E IMPACTO EN EL NEGOCIO.

2.1 Metodología de Análisis y Gestión de Riesgos MAGERIT

Parte importante del Análisis de Riesgos radica básicamente en que va a permitir identificar con claridad las amenazas a las que se encuentran expuestos los diferentes activos de información, pudiendo estimar la frecuencia de materialización de tales amenazas y valorar el impacto al materializarse dicha amenaza.

Teniendo en cuenta que la ISO 27005 no proporciona una metodología en sí de Análisis de Riesgos, sino más bien describe en sus cláusulas todo el proceso recomendado de análisis en donde se incluyen las fases que lo conforman, se hace imprescindible

mencionar a MAGERIT (**M**etodología de **A**nálisis y **GE**stión de **R**iesgos de los Sistemas de **I**nformación de las adminis**T**raciones públicas) en su versión 3 que es una metodología de análisis y gestión de riesgos, elaborada por el Consejo superior de Administración Electrónica CSAE de España, la cual facilita la gestión de los riesgos, esta metodología fue concebida en función del creciente uso de las tecnologías por parte de la sociedad y las organizaciones que permiten conseguir el cumplimientos de sus objetivos , sin embargo asociadas a ese beneficio se incorporan ciertos riesgos que deben minimizarse, y poder establecer una adecuada gestión de los riesgos es de suma importancia [6].

La metodología está incorporada en 3 libros que son:

1. Método: Describe la estructura que debe tener el modelo de gestión de riesgos acorde a lo que propone ISO para la gestión de riesgos, contiene consejos y aspectos prácticos lo cual facilita esta tarea.
2. Catálogo de Elementos: Prácticamente es una especie de inventario, en donde se establecen los activos de información y características que deben tomarse en cuenta al momento de valorarlos, junto con un listado de amenazas y controles, además nos indica cómo desarrollar un informe.

3. Guía de Técnicas: Describe técnicas utilizadas en el análisis de riesgos y ejemplos con tablas, algoritmos, árboles de ataque, análisis de costo beneficio, diagramas de flujo y buenas prácticas.

La metodología de Magerit cabe perfectamente dentro de la Implementación de la gestión de riesgos expresada en la Norma ISO 31000 (Figura 2.1), a lo que se "denomina "Proceso de Gestión de los Riesgos", sección 4.4 ("Implementación de la Gestión de los Riesgos") dentro del "Marco de Gestión de Riesgos" [6].

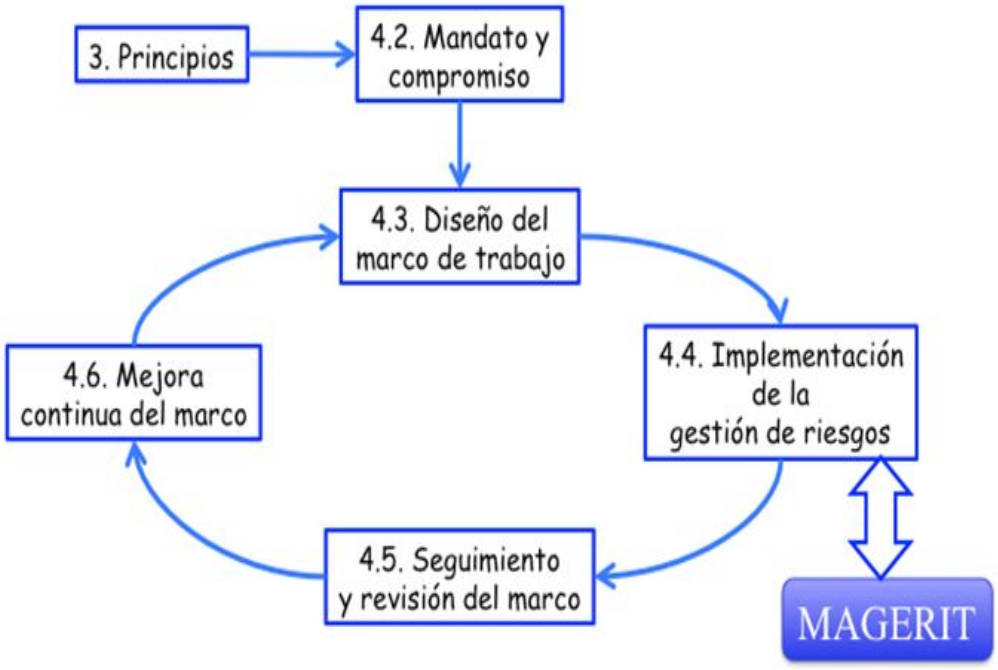


Figura 2.1. ISO 31000 - Marco de trabajo para la gestión de riesgos

Fuente: (Ministerio de Hacienda y Administraciones Públicas España, 2012) MAGERIT v3, Libro I Método

Los objetivos de MAGERIT son:

Directos:

1. Concienciar sobre la existencia de riesgos y gestionar medidas adecuadas para limitar su impacto.
2. Entregar un método sistemático para analizar los riesgos.
3. Descubrir y planificar las medidas necesarias y oportunas para mantener bajo control los riesgos identificados.

Indirectos:

1. Acondicionar y proyectar a la organización en futuros procesos de evaluación, auditoría, certificación o acreditación, en caso de así requerirlo.

Con una visión en conjunto MAGERIT afronta 2 tareas importantes que permiten definir claramente un proceso de Gestión de Riesgos, siendo el Análisis y el Tratamiento del riesgo (Figura 2.2 y 2.3).

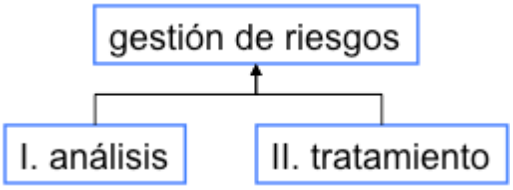


Figura 2.2. Gestión de Riesgos

Fuente: (Ministerio de Hacienda y Administraciones Públicas España, 2012) MAGERIT v3, Libro I Método

Donde el Análisis establece los siguientes elementos:

1. Activos: Todos los elementos que forman parte del Sistema de Información y que soportan la misión de la Organización.
2. Amenazas: Todo incidente no deseado sobre el activo, que provoca un daño y perjuicio a la Organización.
3. Salvaguardas: Implementación de medidas que eviten que las amenazas no causen mucho daño.

En base a estos elementos se pueden estimar:

1. El impacto: Lo que podría producir.
2. El riesgo: Probabilidad de que pase.

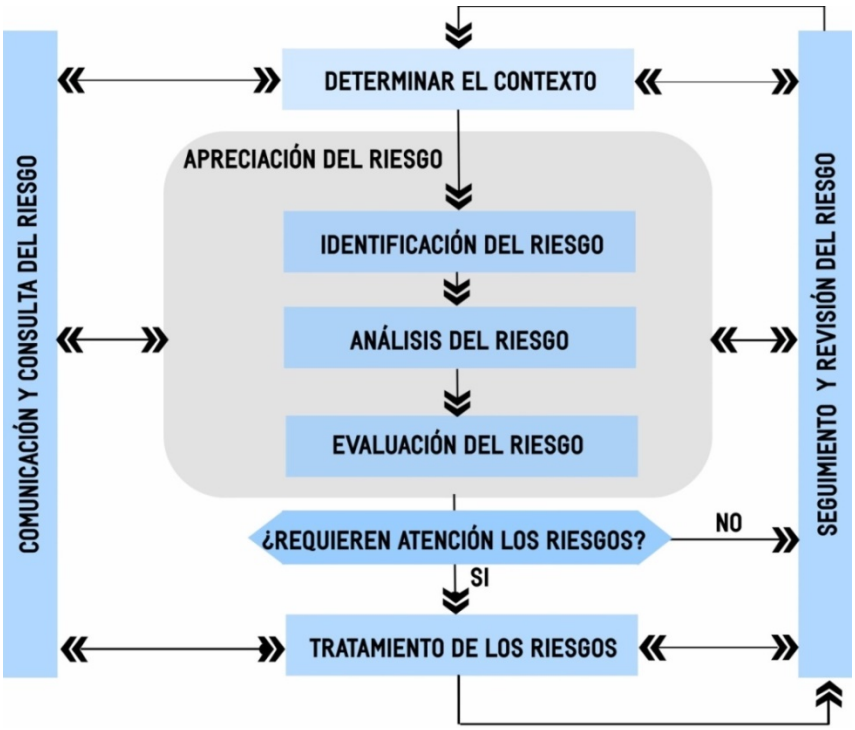


Figura 2.3. Proceso de gestión de riesgos

Fuente: (Ministerio de Hacienda y Administraciones Públicas España, 2012) MAGERIT v3, Libro I Método

Elaborado por: Alfredo Carpio

2.2 EAR (Entorno para el Análisis de Riesgos)

El Centro Cristológico Nacional de España ha desarrollado como un complemento de MAGERIT una herramienta informática para facilitar el análisis y gestión de riesgos, conocida como PILAR (**P**ROCEDIMIENTO **I**NFORMATICO Y **L**OGICO DE **A**NALISIS DE **R**IESGOS) o EAR (**E**ntorno de **A**nálisis de **R**iesgos) estas herramientas cambian solo por el nombre ya que son las mismas la

única diferencia radica en que la primera es de uso privado para el Centro Nacional de Inteligencia y los ministerios de España, en cambio la segunda es de tipo comercial es decir de pago, lo que permitirá obtener resultados automatizados y relevantes, entonces se puede afirmar con certeza que EAR está basada en PILAR.

Objetivo de EAR/PILAR:

1. Facilidad de uso: Permitir un análisis de riesgos intuitivo en un corto espacio de tiempo usuarios inexpertos [7].
2. Flexibilidad: Posibilidad de aptarse a requerimientos de las normativas existentes como ISO.
3. Priorización salvaguardas: Para evitar daños graves.

La herramienta EAR/PILAR permite el análisis y la gestión de riesgos de un sistema de información acorde a la metodología MAGERIT, además dispone de una biblioteca estándar de propósito general, y pudiendo realizar calificaciones de seguridad respecto de normas ampliamente conocidas como [7]:

1. Esquema Nacional de Seguridad de España.
2. ISO/IEC 27002:2005.

3. Los Criterios de Seguridad, Normalización y Conservación España.
4. LOPD Ley Orgánica de Protección de Datos de Carácter Personal España.
5. NIST SP 800-35.
6. COBIT

Toma en cuenta la duración de la interrupción sobre los servicios y sus interrupciones.

2.3 Identificar los procesos críticos del negocio

Para abordar con claridad y exactitud e identificar los procesos críticos del negocio, es necesario entender adecuadamente la organización y su contexto, identificar los productos y servicios claves, para el efecto se ha realizado entrevistas con la Alta Gerencia y mandos altos y medios de tal manera de poder identificar y establecer en base a su conocimiento y experiencia de la organización, cuales son los procesos y recursos que se ven involucrados en la entrega del o los productos o servicios.

Preguntas sencillas y claras se han realizado con el fin de comprender a la organización y determinar cuan urgente sus actividades y procesos deberán ser restablecidos en caso de una disrupción y pérdida de los productos o servicios que entrega a sus clientes.

A continuación el listado de preguntas realizadas a la Alta Gerencia en su orden:

1. ¿Posee la organización un plan de continuidad de negocio o un plan de contingencias informáticas?
2. ¿Teniendo en cuenta la visión, misión y objetivos de la organización, cómo estos objetivos son obtenidos?
3. ¿Cuál o cuáles son los productos o servicios que la organización provee o entrega?
4. ¿Cuál o cuáles a su criterio son los procesos críticos del negocio?
5. ¿Quiénes (Área/persona) son los dueños/responsables de los procesos críticos del negocio?

6. ¿Cuál es el tiempo máximo (minutos, horas, días, semanas) tolerable, en que un determinado impacto impida que la organización entregue los productos o servicios?

Entendiendo la organización y su contexto

Es de vital importancia conocer y entender en modelo de negocio y el entorno de la organización, tomando en cuenta todo aquello que pueda condicionar el lograr los objetivos del negocio.

Descripción del negocio

La Unidad de Negocio Hidropaute forma parte de la Empresa Pública Estratégica Corporación Eléctrica del Ecuador CELEC EP, con sede administrativa ubicada en la Ciudad de Cuenca provincia del Azuay Panamericana Norte Km 7, dedicada a la generación de energía eléctrica, producto del plan estratégico de la compañía se establecieron su misión, visión, objetivos y valores, los cuales están orientados a que Hidropaute sea una empresa líder en el mercado eléctrico del país, posee certificación en normativas internacionales de Gestión de Calidad ISO 9001, Gestión Ambiental ISO 14001, y el estándar para la Gestión de Seguridad y Salud Ocupacional OHSAS 18001.

Infraestructura organizativa

Hidropaute, además de su sede administrativa en Cuenca tiene dos plantas de generación ubicadas en Arenales (Proyecto Integral Paute-Mazar) y Guarumales (Proyecto Integral Paute-Molino) situadas a 140Km de Cuenca y aguas abajo en fases de construcción y estudio el proyecto Sopladora y Cardenillo respectivamente Figura 2.4.

Figura 2.4. Ubicación proyectos de generación Hidropaute

Fuente: http://www.eltiempo.com.ec/noticias-cuenca/82418

Proyecto Mazar

Inicio su operación en el año 2010 y cuenta con 2 unidades de generación de 85MW c/u que dan un total de 170 MW de capacidad con una energía media de 800 GWh/año, cuenta con un embalse de trecientos diez millones de metros cúbicos de volumen útil.

Proyecto Molino

Se encuentra aguas abajo del Proyecto Mazar, inicio su operación en el año 1983 y cuenta con 10 unidades de generación, 5 unidades fase AB 500 MW y 5 unidades fase C 575MW con un total de 1075 MW de capacidad, tiene un embalse para almacenar 120 millones de metros cúbicos de agua, actualmente cuenta 80 millones de metros cúbicos de volumen útil.

La infraestructura de sistemas

En la Figura 2.5 se puede observar los tipos y elementos que forman parte de las conexiones entre el sitio administrativo y las plantas de producción.

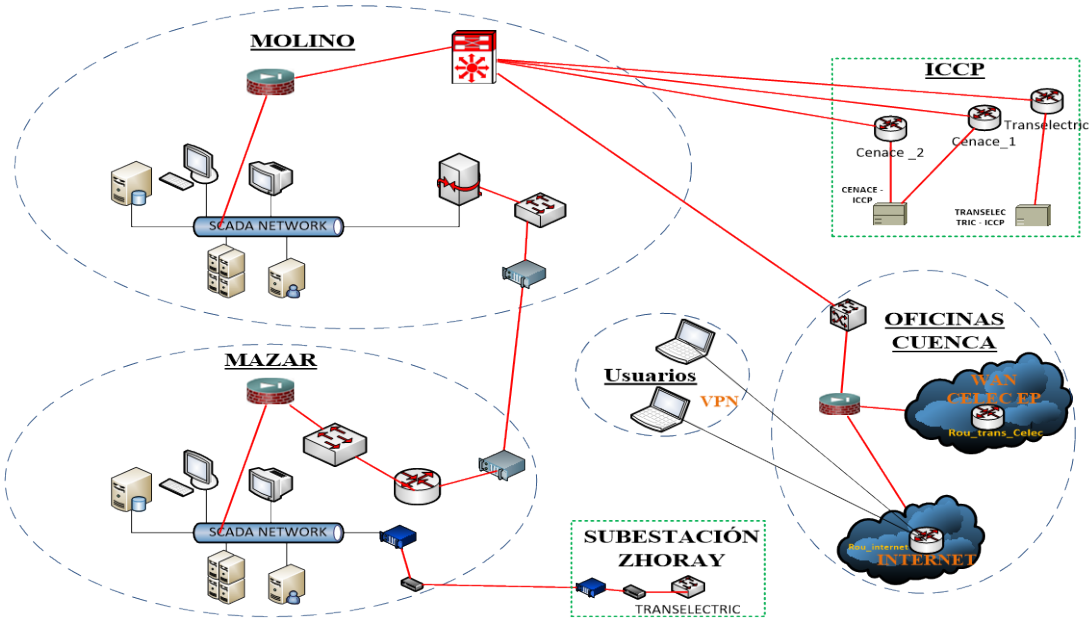


Figura 2.5. Red Corporativa Hidropaute

Fuente: Hidropaute

Elaborado por: Alfredo Carpio

La conexión a internet, es proporcionada por el ISP de TRANSNEXA (Transelectric) corresponde tanto a salida a Internet para todos las sitios como para la conexión VPN (Virtual Private Network) de los funcionarios que acceden a la red de la organización.

Organigrama

La estructura jerárquica de la organización se muestra en el organigrama presente en la Figura 2.6, donde se establece claramente las áreas funcionales de la empresa.

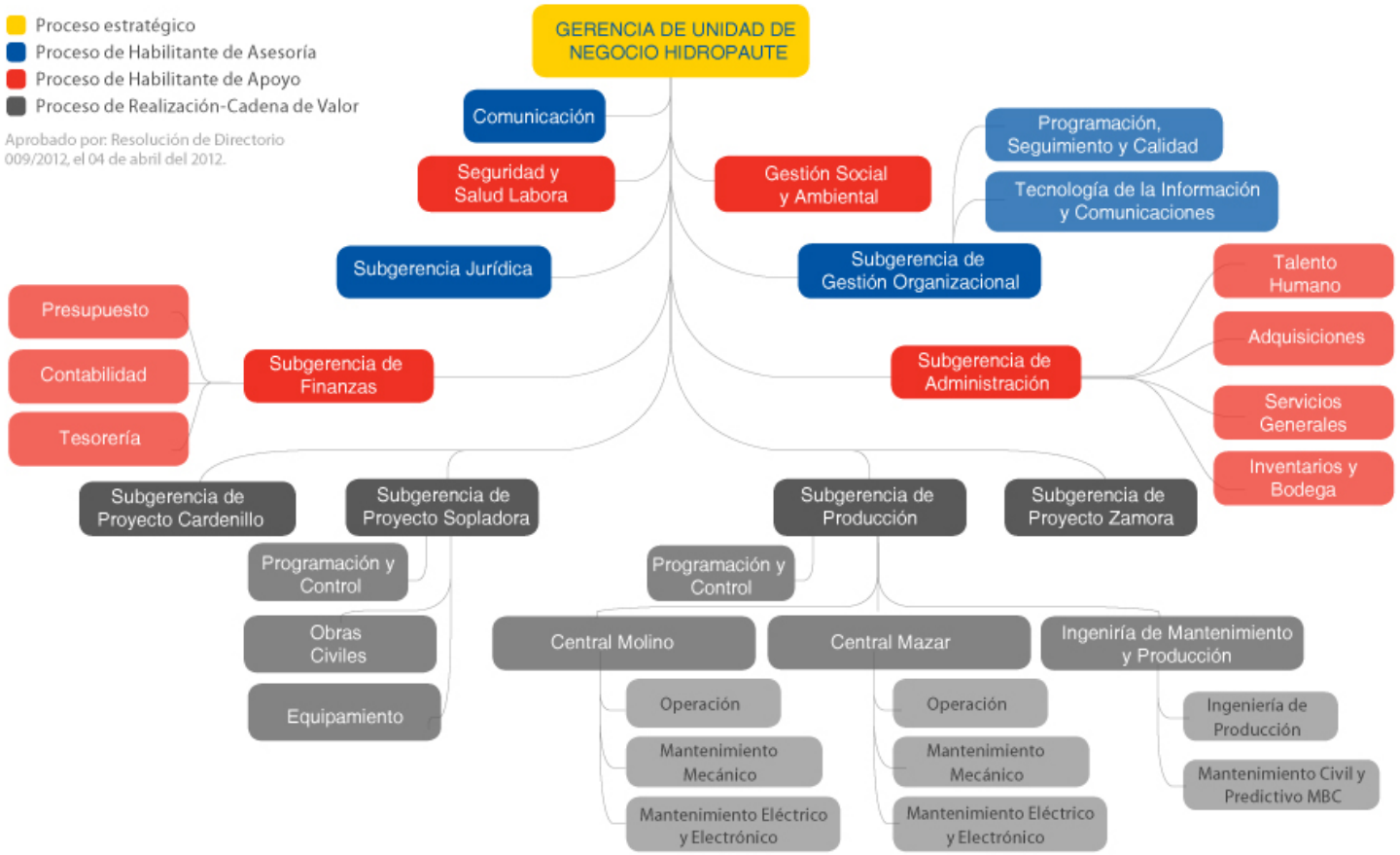


Figura 2.6. Estructura Organizacional Hidropaute

Fuente: Hidropaute

Análisis externo

La unidad de Negocio Hidropaute es parte de la Corporación Eléctrica del Ecuador CELEC EP que es una Empresa Pública y por su ámbito de acción, se la define como un servicio público estratégico, se creó mediante Decreto Ejecutivo No. 220, expedido el 14 de Enero del 2010.

La Constitución de la República del Ecuador en su Artículo 314, establece que “El Estado es responsable de la provisión de servicio eléctrico y éste debe responder a los “principios de obligatoriedad, generalidad, uniformidad, responsabilidad, universalidad, accesibilidad, regularidad, continuidad y calidad” [8].

Además en el Artículo 315, establece que “El Estado constituirá empresas públicas para la gestión de sectores estratégicos, la prestación de servicios públicos, el aprovechamiento sustentable de recursos naturales o de bienes públicos y el desarrollo de otras actividades económicas” [8].

Una de las principales actividades de CELEC EP es “La generación, transmisión, distribución, comercialización, importación y

exportación de energía eléctrica” [8], para el efecto Hidropaute es parte del conjunto de unidades de negocio hidráulicas (Figura 2.7) que se dedica a generar energía eléctrica mediante fuentes renovables, de acuerdo al concepto de energía renovable “es aquella que se obtiene de fuentes naturales virtualmente inagotables, ya sea por la inmensa cantidad de energía que contienen, o porque son capaces de regenerarse por medios naturales. Entre las energías renovables se cuentan la eólica, geotérmica, hidroeléctrica, mareomotriz, solar, undimotriz, la biomasa y los biocombustibles” [9].

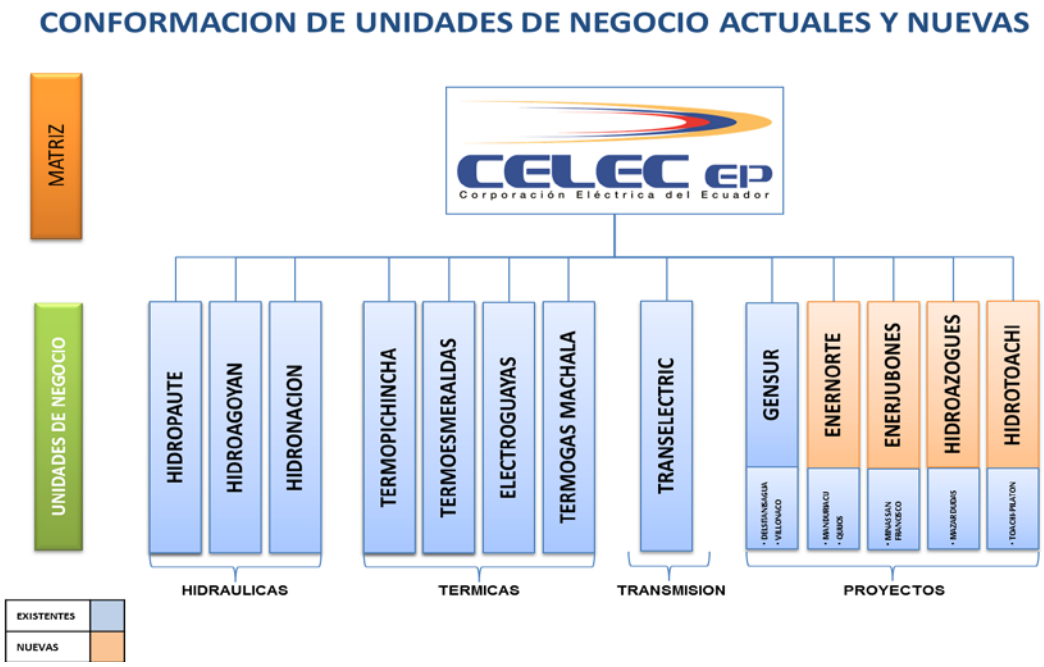


Figura 2.7. Unidades de Negocio actuales y nuevas de CELEC EP

Fuente: CELEC EP

Dentro del ámbito de Hidropaute existen partes interesadas las cuales se presentan en la Figura 2.8, todas estas tienen expectativas:

1. Accionistas
    - ✓ Apoyo a cambio de Matriz Energética.
    - ✓ Eficacia, Eficiencia.
    - ✓ Minimizar perdidas y Maximizar ganancias.
2. Administración
    - ✓ Información oportuna y transparente.
    - ✓ Eficacia y eficiencia.
3. Servidores
    - ✓ Bienestar y desarrollo laboral.
4. Clientes
    - ✓ Energía, confiabilidad y disponibilidad.
    - ✓ Información oportuna y transparente.
5. Contratistas
    - ✓ Cumplimiento de contrato.
    - ✓ Atención oportuna.
    - ✓ Comportamiento ético.
6. Estado

- ✓ Cumplimiento legal.
- ✓ Atención oportuna.
- ✓ Comportamiento ético.

7. Ambiente
    - ✓ Prevención de contaminación y uso eficiente de recursos.
    - ✓ Preservación y restauración de la biodiversidad.
    - ✓ Cumplimiento legal.
    - ✓ Transparencia y comportamiento ético.
8. Comunidades y Sociedad
    - ✓ Atención cordial y oportuna.
    - ✓ Servicios de calidad.
    - ✓ Contribuir al desarrollo de las comunidades.
    - ✓ Cumplimiento de acuerdos.
    - ✓ Apoyo a desarrollo profesional (tesis, prácticas, educación y capacitación).
    - ✓ Comunicación e información oportuna y transparente.
    - ✓ Cumplimiento legal, eficacia y eficiencia.

Figura 2.8. Partes Interesadas Hidropaute

Fuente: Hidropaute

Análisis interno

Este análisis permite visualizar con claridad cómo están alineados los diferentes procesos para conseguir los objetivos de la organización, su visión, misión, cadena de valor, productos o servicios que ofrece al mercado, los procesos que lo soportan y recursos que se utilizan en esos procesos Figura 2.9.

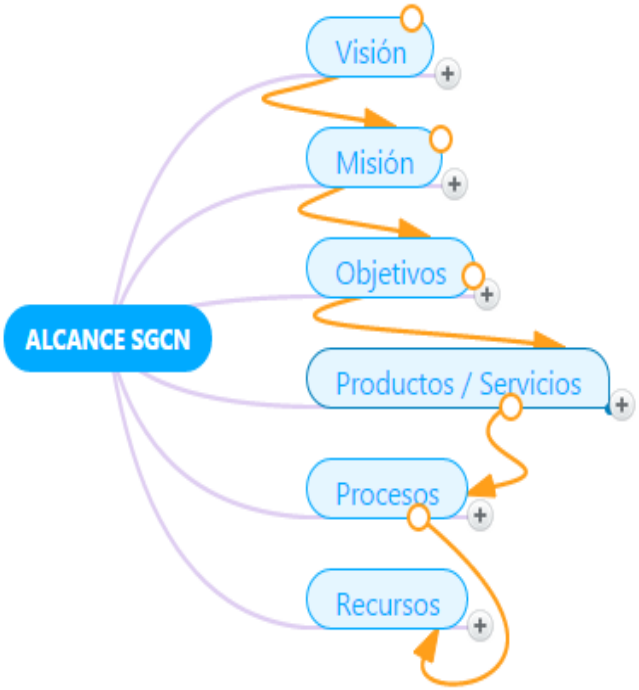


Figura 2.9. Alcance Sistema de Gestión Continuidad del Negocio

Fuente: ISEC-Information Security Inc. [10]

Elaborado por: Alfredo Carpio

Visión

"Ser la Empresa pública líder que garantiza la soberanía eléctrica e impulsa el desarrollo del Ecuador" [11].

Misión

"Generar bienestar y desarrollo nacional como la mayor generadora de CELEC EP, mediante la ejecución de proyectos y la provisión de energía eléctrica de fuentes renovables, con altos estándares de

calidad y eficiencia, responsabilidad social y el aporte de su talento humano altamente comprometido y competente, respetando y protegiendo el ambiente" [11].

Objetivos generales de la organización

1. "Incrementar la disponibilidad y confiabilidad del Sistema Eléctrico Nacional bajo estándares de calidad, eficiencia, eficacia y responsabilidad social" [11].
2. "Incrementar la oferta del servicio eléctrico para abastecer la demanda con responsabilidad social, mejorar la reserva, ampliar la cobertura y contribuir al cambio de la matriz energética" [11].
3. "Incrementar la eficiencia institucional" [11].
4. "Incrementar el desarrollo del Talento Humano" [11].
5. "Incrementar la sustentabilidad Financiera" [11].

Identificación de la Cadena de Valor

La cadena de valor de Hidropaute se expresa en el mapa de procesos (Figura 2.10) de donde más adelante se podrá definir el o los procesos críticos de la organización.

Los procesos agregadores de valor de Hidropaute son:

1. Expansión en Infraestructura de Generación: Estudios, diseños, construcción.
2. Disponibilidad de Planta: Mantenimiento.
3. Generación de Energía: Operación.
4. Despacho y liquidación energética: Liquidación energía producida.

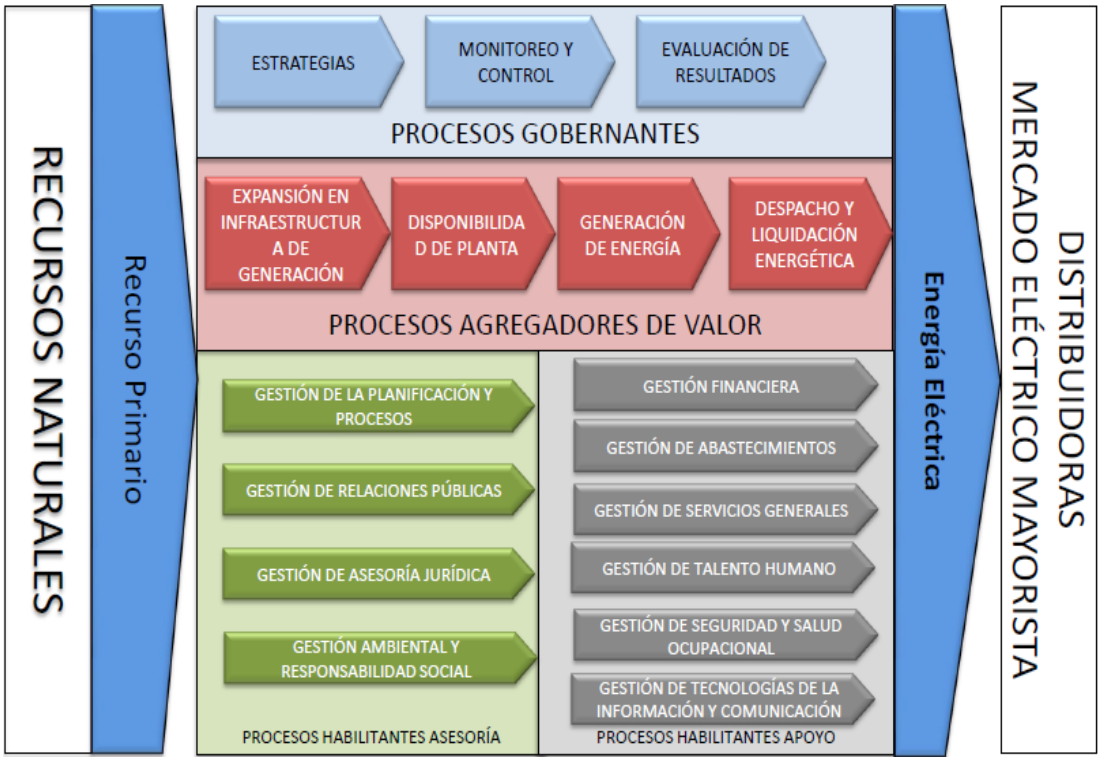


Figura 2.10. Mapa de procesos Unidad de Negocio Hidropaute

Fuente: Hidropaute

Identificación de los Productos y Servicios Claves

En la misión de la organización se establece claramente que Hidropaute está comprometida con la “provisión de energía eléctrica de fuentes renovables” y uno de sus Objetivos es “Incrementar la disponibilidad y confiabilidad del Sistema Eléctrico Nacional” (11), tomando en cuenta estas premisas en las entrevistas realizadas a la Alta Gerencia se destaca de manera diáfana que el producto o servicio que ofrece al mercado y que permiten alcanzar los objetivos es la entrega de energía eléctrica (Tabla 1).

Tabla 1. Productos o servicios

Productos / Servicio	**Descripción del Producto o Servicio**
Energía eléctrica	Electricidad producida con energía renovable

Fuente: Entrevistas Alta Gerencia

Elaborado: Alfredo Carpio

Identificar los tiempos imperativos de entrega del Producto y Servicio Clave

BIA – Business Impact Analysis

El BIA, analiza cada producto o servicio, proceso y actividad dentro de la organización, entiende el significado para la organización y determina los impactos que resultarían de una interrupción en un cierto tiempo, determina en qué momento en el tiempo se vuelve intolerable (después de una interrupción), Esto se llama “Periodo Máximo Tolerable de Interrupción MTPoD” Figura 2.11.

Se identifica para el efecto 3 tipos de BIA:

1. **Estratégico: Perdidas de Productos y Servicios (P y S)**

   En este punto la Alta Gerencia determina el Impacto con tiempo sobre la organización de una interrupción del producto o servicio que se entrega, que en este caso es la energía eléctrica, cuyo alcance de este estudio es la Central Paute-Mazar.

   Hidropaute dentro de sus metas para el año 2014 tiene declarado valores de disponibilidad y confiabilidad, es así

que para la central Paute-Mazar (Tabla 2), se tiene proyectada una disponibilidad anual (8760 Horas) de 95,15% lo cual da un promedio anual de indisponibilidad de 4,85% que representa al año 424,86 horas, debiendo tomar en cuenta además que las unidades entran en un plan de mantenimiento programado cada ocho mil horas lo cual implica una indisponibilidad programada de 239 horas (196 horas unidad en mantenimiento y 43 horas unidad que no está en mantenimiento, de acuerdo a valores estadísticos registrados en el último mantenimiento) cada 1,5 años es decir alrededor de 159,33 horas al año por unidad, que dan en total de 318,66 horas.

En consecuencia un evento de indisponibilidad no programado en el año puede ser de no más de 106,2 horas para alcanzar la meta propuesta por Hidropaute.

Horas de indisponibilidad anual:

424,86 – 318,66 = **106,2 horas**

Horas de indisponibilidad mensual:

106,2 / 12 = **8,85 horas**

Esto significa que uno o más eventos que provoque indisponibilidad en el mes sumado no pueden durar más de 8,85 horas o 8 horas 51 minutos.

Tabla 2. Metas Disponibilidad 2014 Paute-Mazar

HIDROPAUTE METAS ESTRATEGICAS 2014	
CENTRAL MAZAR	
MES	DISPONIBILIDAD
ENERO	77,92
FEBRERO	98,48
MARZO	98,62
ABRIL	98,58
MAYO	98,62
JUNIO	98,58
JULIO	98,62
AGOSTO	98,62
SEPTIEMBRE	98,58
OCTUBRE	77,92
NOVIEMBRE	98,58
DICIEMBRE	98,62
ANUAL	**95,15**

Fuente: Hidropaute

Elaborado: Alfredo Carpio

Hasta Noviembre del año 2014 se han presentado 24 eventos que han causado la interrupción de la entrega de energía y por ende indisponibilidad de la planta ver Anexo A.

En consecuencia de los datos presentados como antecedentes, la Alta Gerencia podría determinar que para un evento de indisponibilidad promedio al mes el MTPoD será de 8 horas 51 minutos, tomando en cuenta que en el transcurso del año 2014 (Enero-Octubre= 10 meses) los datos estadísticos indican que existieron 24 interrupciones en 10 meses (24/10= 2,4 veces) se puede decir que hay un promedio de incidentes de más o menos 2 veces al mes, cada evento en consecuencia deberá ser no mayor a 4,425 horas (**4 horas 25 minutos**), lo cual permitirá la entrega del producto o servicio en los valores pactados de potencia hacia su cliente, manteniendo así las metas propuestas por la organización.

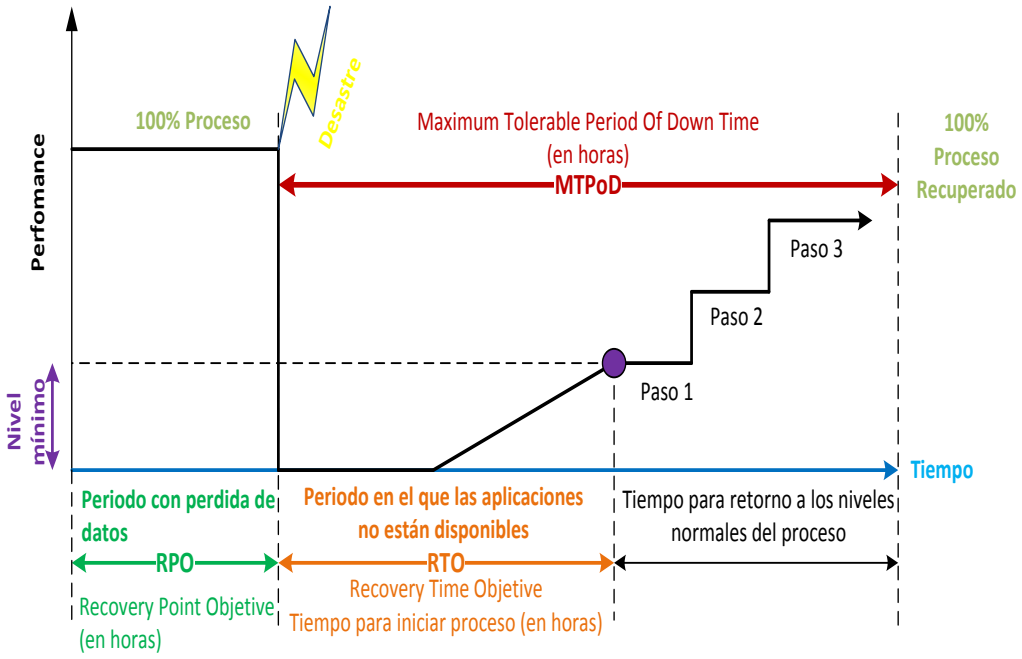


Figura 2.11. MTPoD

Fuente: ISEC-Information Security Inc. [10]

Elaborado: Alfredo Carpio

Cálculo del costo que implica dejar de entregar el servicio

Basados en el MTPoD y teniendo en cuenta que a la organización le impacta en el aspecto económico se puede determinar el valor que deja de percibir la organización por dejar de entregar el producto, para el cálculo utilizaremos los

siguientes ejemplos con datos proporcionados por Hidropaute:

- ✓ **Consideraciones**

  CENACE paga a Hidropaute por dos rubros a saber:

  - o **Cargo fijo:** El valor del cargo fijo se paga en base a la disponibilidad de las unidades de generación de la Central Paute-Mazar. Es decir se paga por la potencia en Megavatios (MW) disponible de las unidades, estén generando o estén en reposo. Para esto calculan una disponibilidad promedio de los últimos 12 meses y si dicho promedio es mayor al 90% pagan el total del monto asignado por cargo fijo. Si dicho promedio es menor al 90% el CENACE paga el proporcional del monto total asignado. Para la Central Paute-Mazar el monto mensual asignado si se iguala o supera el 90% de disponibilidad promedio de los últimos 12 meses es de $ 1.162.185,68 dólares americanos.

- **Cargo variable**: El valor del cargo variable se paga en base a la generación de las unidades de la Central Paute-Mazar. Es decir se paga por la energía Megavatios hora (MWh) generada. El CENACE se encarga de indicar al centro de control de Paute-Mazar cuanto tiene que generar, a esto se le llama el despacho de generación del CENACE. Hidropaute comercializa a 0.02 centavos de dólar americanos el Kilovatio hora, este valor en MWh representa $2 dólares americanos.

✓ **Cálculo de costos**

En la Tabla 3 se encuentran los porcentajes de disponibilidad mensual de los últimos 11 meses (Junio 2014 – Abril 2015) y el cálculo de disponibilidad promedio (94,32%) de los mismos que da un valor superior al 90%.

Tabla 3. Disponibilidad mensual Paute-Mazar (Junio 2014 – Abril 2015)

MESES	DISPONIBILIDAD
abr-15	78.17%
mar-15	87.05%
feb-15	95.48%
ene-15	99.79%
dic-14	99.63%
nov-14	99.98%
oct-14	100.00%
sep-14	100.00%
ago-14	77.76%
jul-14	99.73%
jun-14	99.88%
PROMEDIO	**94.32%**

Fuente: Hidropaute

Elaborado: Alfredo Carpio

- **Calculo cargo fijo**

  Si la indisponibilidad fuese de 8 horas 51 minutos, las pérdidas de generación en un mes no afectan significativamente a la disponibilidad promedio de los últimos 12 meses. Como ejemplo, en el mes de abril 2015, la Unidad 1 de Mazar entró en mantenimiento mayor (8000 horas de operación) por 196 horas aproximadamente y la U2 alrededor de 43 horas, bajó la disponibilidad al 78.17%. Al promediar con los otros meses aún se obtiene

una disponibilidad promedio superior al 90%. Por lo tanto si el mes de mayo 2015 se pierde 8 horas 51 minutos como es el caso de este ejemplo no es significativo, por lo tanto se considera que se pagará el monto total del cargo fijo.

Sin embargo si las fallas se repitiesen de manera constante empezaría a disminuir el porcentaje de disponibilidad y en consecuencia Hidropaute empieza a recibir menos ingresos por cargo fijo de acuerdo a Tabla 4:

Tabla 4. Pago por cargo fijo

Pago por cargo fijo		
Porcentaje Disponibilidad	**Cobraría**	**Dejaría de cobrar**
90	1162185.68	0.00
89	1149272.51	12913.17
88	1136359.33	25826.35
87	1123446.16	38739.52
86	1110532.98	51652.70
85	1097619.81	64565.87
84	1084706.63	77479.05

83	1071793.46	90392.22
82	1058880.29	103305.39
81	1045967.11	116218.57
80	1033053.94	129131.74
79	1020140.76	142044.92
78	1007227.59	154958.09
77	994314.42	167871.26
76	981401.24	180784.44
75	968488.07	193697.61
74	955574.89	206610.79
73	942661.72	219523.96
72	929748.54	232437.14
71	916835.37	245350.31
70	903922.20	258263.48
69	891009.02	271176.66
68	878095.85	284089.83
67	865182.67	297003.01
66	852269.50	309916.18
65	839356.32	322829.36
64	826443.15	335742.53
63	813529.98	348655.70
62	800616.80	361568.88
61	787703.63	374482.05
60	774790.45	387395.23
59	761877.28	400308.40
58	748964.10	413221.58
57	736050.93	426134.75
56	723137.76	439047.92
55	710224.58	451961.10
54	697311.41	464874.27
53	684398.23	477787.45
52	671485.06	490700.62
51	658571.89	503613.79
50	645658.71	516526.97
49	632745.54	529440.14
48	619832.36	542353.32
47	606919.19	555266.49
46	594006.01	568179.67
45	581092.84	581092.84

Fuente: Hidropaute

Elaborado: Alfredo Carpio

- **Calculo cargo variable**

  El despacho del CENACE estaba coordinado para que la U1 y U2 de Mazar funcionen de manera continua las próximas 24 horas a 85 MWh cada una, que es la potencia máxima que generan las unidades.

  En ese período de 24 horas se produce una incidencia que provoca la paralización de la entrega de energía eléctrica total en las unidades por 8 horas 51 minutos, lo cual provoca una pérdida de $ 1504,50 dólares americanos tal cual se refleja en la Tabla 5 y Tabla 6.

Tabla 5. Pérdidas en el cargo variable por 1 hora c/unidad

Unidad	Potencia (MW)	Tiempo (h)	Energía (MWh)	Costo MWh ($)	Pérdida ($)
U1	85.00	1.00	85.00	2.00	170.00
U2	85.00	1.00	85.00	2.00	170.00
CENTRAL	170.00	1.00	170.00	2.00	**340.00**

Fuente: Hidropaute

Elaborado: Alfredo Carpio

Tabla 6. Pérdidas en el cargo variable por 8 horas 51 minutos

Unidad	Potencia (MW)	Tiempo (h)	Energía (MWh)	Costo MWh ($)	Pérdida ($)
U1	85.00	4.425	376.13	2.00	752.25
U2	85.00	4.425	376.13	2.00	752.25
CENTRAL	170.00	8.85	752.25	2.00	**1504.50**

Fuente: Hidropaute

Elaborado: Alfredo Carpio

2. **Táctico: Interrupción de Procesos y Subprocesos**

   En este ámbito se determina el Impacto en umbrales de tiempo de la pérdida de cada proceso en la capacidad de entregar el servicio de energía eléctrica.

Luego de las entrevistas y reuniones con la Alta gerencia se determina que el Macroproceso “Generación de Energía” es el más crítico y dado que este plan de contingencia aplica al proyecto de generación hidroeléctrica Paute-Mazar, nos enfocamos al proceso crítico “Operación Central Mazar” que apalanca los objetivos estratégicos de la organización (Figura 2.12).

1. Proceso	OPERACIÓN DE CENTRAL MAZAR	3. Macro	GENERACIÓN DE ENERGÍA
2. Responsable	JEFE DE OPERACIÓN	4. Tipo	AGREGADORES DE VALOR
5. Propósito:	Planificar, organizar y controlar la operación de central Paute-Mazar a fin de asegurar la continua y eficiente generación de energía eléctrica bajo los estándares de calidad y requisitos legales vigentes.		

6. Proveedores Principales	7. Controles		8. Clientes Principales
MANTENIMIENTO TIC HIDROLOGÍA	Despacho de carga diario Límites Operativos Legislación del sector eléctrico	Instructivos de operación Políticas operativas	CENACE LIQUIDACIÓN ENERGÉTICA MANTENIMIENTO

9. Entradas y Salidas

- Recurso hídrico - Programa semanal de intervenciones -Plan anual de indisponibilidad -Pronóstico de caudales - Solicitud apertura desagüe de fondo	OPERACIÓN CENTRAL MAZAR	- Recurso hídrico regulado - Energía eléctrica y servicios complementarios - Reporte de equipo defectuoso - Reporte de medición comercial

10. Recursos especiales

SCADA, GMS y comunicaciones Instalaciones electromecánicas y civiles	Manuales del fabricante y planos

11. Subproceso	12. Actividades
PLANIFICACIÓN DE OPERACIÓN DE CENTRAL MAZAR	Planificación operativa a mediano plazo - Programación de ingreso y salida de unidades - Programación de Monitoreo de la Central
OPERACIÓN DE CENTRAL MAZAR	Operación en Tiempo Real - Consignación y Recepción de sistemas y Equipos - Monitoreo
ANÁLISIS POST-OPERATIVO	Procesamiento de Datos Operativos y de Monitoreo - Análisis de Datos y Elaboración de Informes

Figura 2.12. Proceso Operación Central Mazar

Fuente: Hidropaute

Como subprocesos que son parte de la Operación Central Mazar encontramos los siguientes (Figura 2.13).

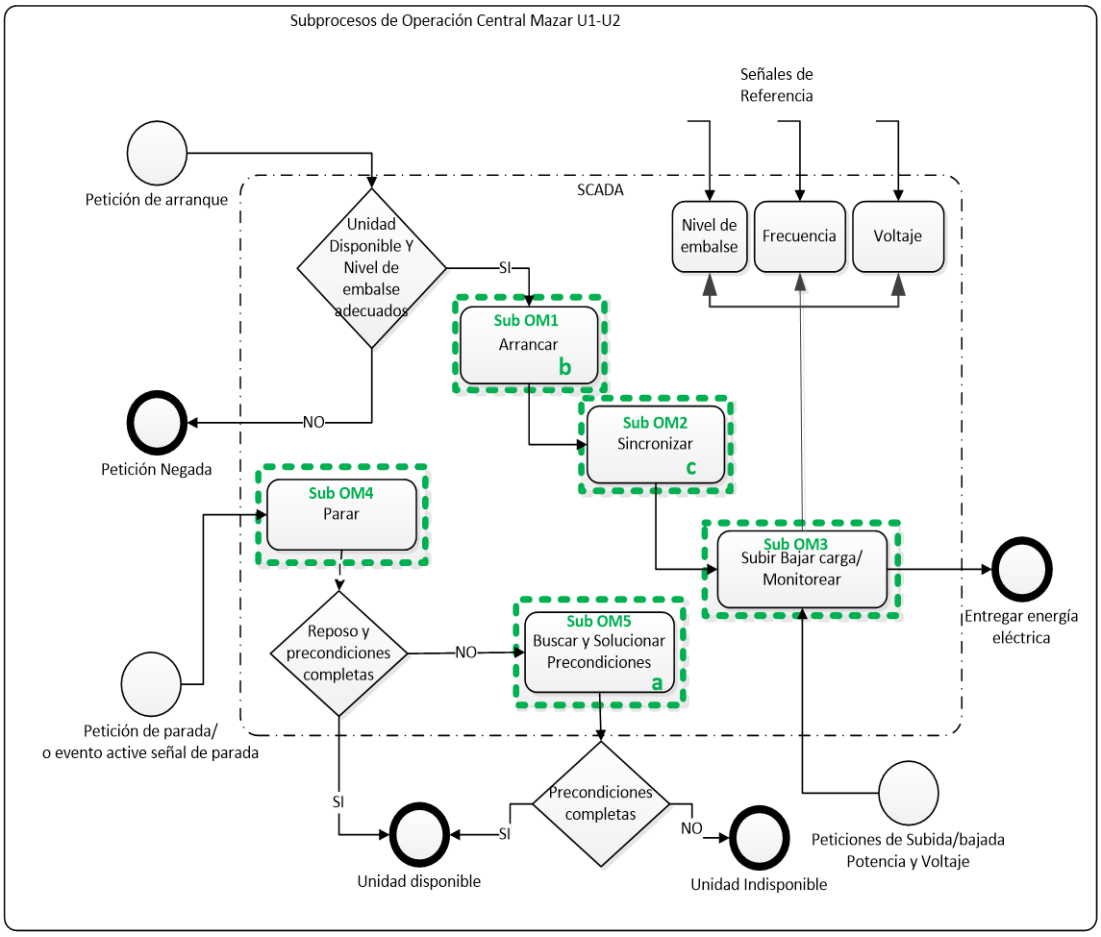


Figura 2.13. Subprocesos Operación Central Mazar

Fuente: Propia

Elaborado: Alfredo Carpio

El tiempo que tome recuperar los subprocesos SubOM5 + SubOM1 + SubOM2 deberá ser <= RTO Proceso (3 horas 30 minutos), tal cual se refleja en la Tabla 7.

Tabla 7. Procesos / Subprocesos que soportan los P/S clave

Identificación de Procesos / Subprocesos que soportan los P/S claves			
P/S clave= Energía Eléctrica			
Proceso	**Subprocesos**	**RTO Subproceso**	**RTO Proceso**
OPERAR CENTRAL MAZAR	SubOM5 Buscar y Solucionar Precondiciones (Mantenimiento)	3 horas	3horas 30minutos
	SubOM1 Arrancar Unidad	25 minutos	
	SubOM2 Sincronizar Unidad	5 minutos	

Fuente: Propia

Elaborado: Alfredo Carpio

3. **Operacional: Interrupciones de los Recursos.**

   Toma en cuenta los recursos (Premises/Instalaciones, Proveedores, Personas, Tecnología, Información, Suministros, Servicios) que los procesos y subprocesos

utilizan para entregar el servicio o producto a sus clientes, En el punto 2.4 Tabla 9 más adelante se identificará los recursos tecnológicos críticos necesarios para la recuperación de los procesos, así como en la Tabla 10 se definen el Período Máximo Tolerable de Interrupción (MTPoD) , el Punto Objetivo de Recuperación (RTO) y el Punto Objetivo de Recuperación electrónica (RPO) .

2.4 Identificar los recursos críticos de TIC, involucrados en los procesos críticos del negocio

Luego de identificar los procesos críticos de la organización, es conveniente identificar que recursos están soportando dichos procesos. En la Tabla 8 se presenta los recursos involucrados en el proceso de Operación Central Mazar, siendo este un plan de contingencia informático el alcance de los recursos se centrarán en la Información (física - electrónica) y Tecnología de TIC involucrado en el mismo.

Tabla 8. Recursos PPPTISS

	RECURSOS	Personas	Tecnología	Información
SUBPROCESOS	**Análisis, Planificación, Reportes**	Operador CENACE, Supervisor Operación, Jefe Operación	• Portátil • Red Corporativa (Email) • Multiplexores • Medidores comerciales ION	• Informes hidrológicos • Informes de falla y salidas Forzadas • Programación Semanal • Consignaciones de Unidades • Mediciones y Liquidaciones comerciales
	Petición de Arranque	Operador CENACE, Operador Sala de Control Molino	• Central telefónica IP, analógico • PLC , Hotline • Red Corporativa (Email) • Multiplexores	
	Arranque	Operador CM, Operador SC	• Central telefónica DECT, analógica, IP • Multiplexores • SCADA, Alspa 320 • Bases de datos	
	Sincronización	Operador SC, Operador CM	• Central telefónica DECT • CCTV • Multiplexores • SCADA, Alspa 320 • Bases de datos	

	Generación	Operador SC, Operador CM	• Central telefónica DECT • CCTV • Multiplexores • SCADA, Alspa 320 • Comunicaciones Sistema Vibraciones • Bases de datos	Datos de Potencia Activa y Reactiva, tensiones, frecuencia, alarmas
	Monitoreo	Operador SC, Operador CM	• Central telefónica DECT, IP • CCTV • Multiplexores • SCADA, Alspa 320 • Comunicaciones Sistema Vibraciones • Comunicaciones Sistema de Protecciones • Comunicaciones Sistema de Descargas Parciales • SCAD / AROCHE • Bases de datos	Datos de Operación en tiempo real como: • nivel de los embalses • potencias de las unidades • Despachos • Redespachos
	Petición de parada	Operador CENACE, Operador Sala de Control Molino	• Central telefónica IP, analógico • PLC , Hotline • Red Corporativa (Email) • Multiplexores	
	Parada	Operador CM, Operador SC	SCADA, alspa 320	
	Precondiciones	Operador CM, Operador SC	• Multiplexores • SCADA, alspa 320	• Datos de Falla • Datos de descargas parciales

Fuente: Propia

Elaborado: Alfredo Carpio

Recursos tecnológicos (activos de información) involucrados

Para el efecto los activos se han dividido en cuatro capas (Figura 2.14).

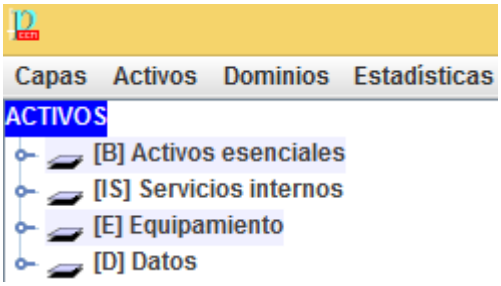


Figura 2.14. Capas de activos

Fuente: Propia

Elaborado: Alfredo Carpio

Los activos de información se han incorporado dentro de estas capas de tal manera que representen un listado de los mismos de manera ordenada (Figura 2.15).

Figura 2.15. Listado de activos de información

Fuente: Propia

Elaborado: Alfredo Carpio

Valoración de los activos

Para la valoración se han tomado en cuenta una escala cualitativa de criterios que va del 0 al 10 (Figura 2.16).

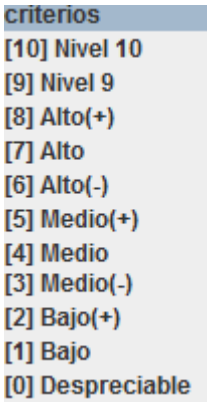
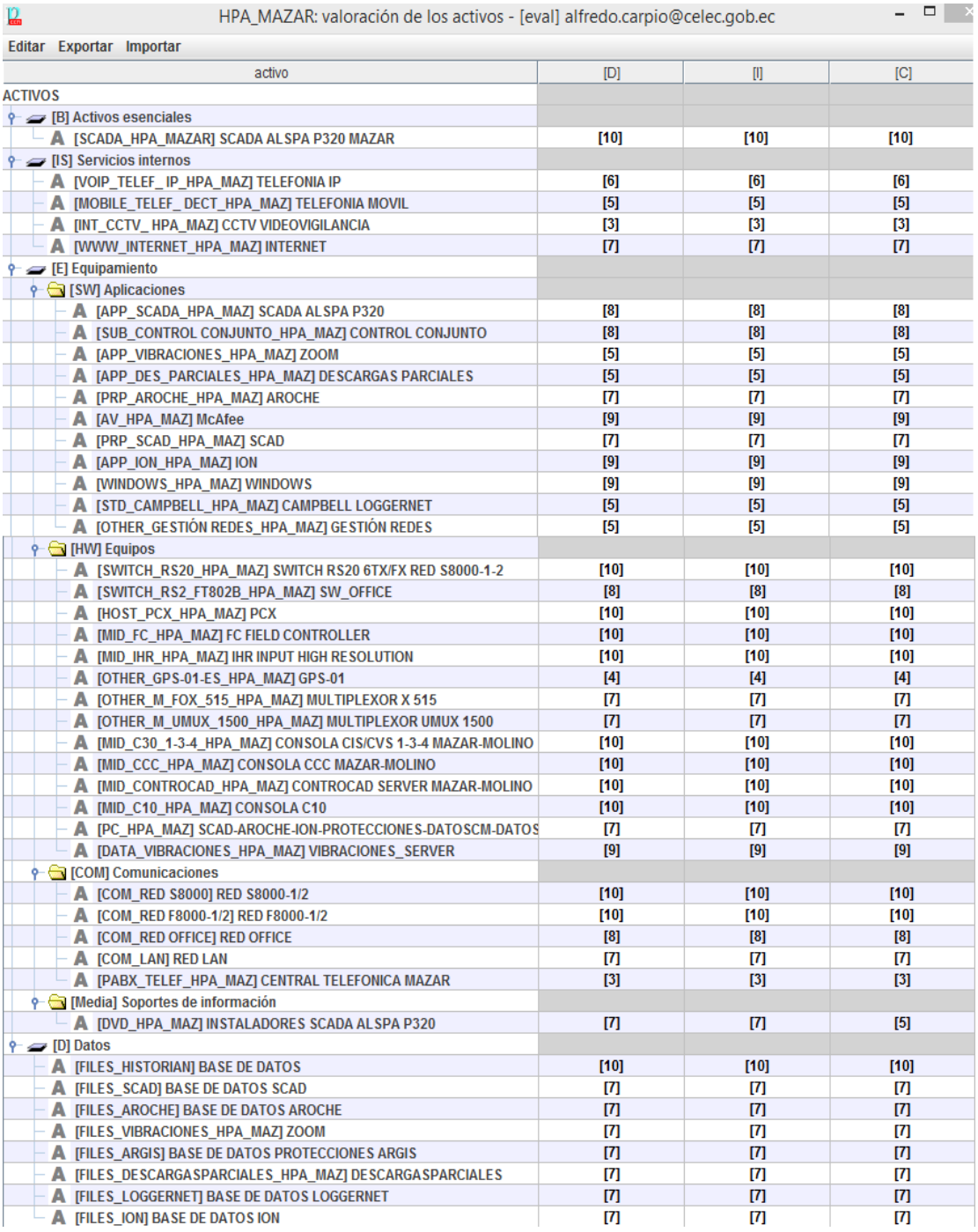


Figura 2.16. Criterios de valoración de activos

Fuente: Propia

Elaborado: Alfredo Carpio

Cada uno de los activos ha sido calificado con los criterios mencionados anteriormente en las dimensiones de Disponibilidad, Confidencialidad e Integridad (Figura 2.17), además se presenta una representación gráfica de tipo araña de la valoración de los activos (Figura 2.18).



HPA_MAZAR: valoración de los activos - [eval] alfredo.carpio@celec.gob.ec

Editar Exportar Importar

activo	[D]	[I]	[C]
ACTIVOS			
[B] Activos esenciales			
[SCADA_HPA_MAZAR] SCADA ALSPA P320 MAZAR	[10]	[10]	[10]
[IS] Servicios internos			
[VOIP_TELEF_ IP_HPA_MAZ] TELEFONIA IP	[6]	[6]	[6]
[MOBILE_TELEF_ DECT_HPA_MAZ] TELEFONIA MOVIL	[5]	[5]	[5]
[INT_CCTV_ HPA_MAZ] CCTV VIDEOVIGILANCIA	[3]	[3]	[3]
[WWW_INTERNET_HPA_MAZ] INTERNET	[7]	[7]	[7]
[E] Equipamiento			
[SW] Aplicaciones			
[APP_SCADA_HPA_MAZ] SCADA ALSPA P320	[8]	[8]	[8]
[SUB_CONTROL CONJUNTO_HPA_MAZ] CONTROL CONJUNTO	[8]	[8]	[8]
[APP_VIBRACIONES_HPA_MAZ] ZOOM	[5]	[5]	[5]
[APP_DES_PARCIALES_HPA_MAZ] DESCARGAS PARCIALES	[5]	[5]	[5]
[PRP_AROCHE_HPA_MAZ] AROCHE	[7]	[7]	[7]
[AV_HPA_MAZ] McAfee	[9]	[9]	[9]
[PRP_SCAD_HPA_MAZ] SCAD	[7]	[7]	[7]
[APP_ION_HPA_MAZ] ION	[9]	[9]	[9]
[WINDOWS_HPA_MAZ] WINDOWS	[9]	[9]	[9]
[STD_CAMPBELL_HPA_MAZ] CAMPBELL LOGGERNET	[5]	[5]	[5]
[OTHER_GESTIÓN REDES_HPA_MAZ] GESTIÓN REDES	[5]	[5]	[5]
[HW] Equipos			
[SWITCH_RS20_HPA_MAZ] SWITCH RS20 6TX/FX RED S8000-1-2	[10]	[10]	[10]
[SWITCH_RS2_FT802B_HPA_MAZ] SW_OFFICE	[8]	[8]	[8]
[HOST_PCX_HPA_MAZ] PCX	[10]	[10]	[10]
[MID_FC_HPA_MAZ] FC FIELD CONTROLLER	[10]	[10]	[10]
[MID_IHR_HPA_MAZ] IHR INPUT HIGH RESOLUTION	[10]	[10]	[10]
[OTHER_GPS-01-ES_HPA_MAZ] GPS-01	[4]	[4]	[4]
[OTHER_M_FOX_515_HPA_MAZ] MULTIPLEXOR X 515	[7]	[7]	[7]
[OTHER_M_UMUX_1500_HPA_MAZ] MULTIPLEXOR UMUX 1500	[7]	[7]	[7]
[MID_C30_1-3-4_HPA_MAZ] CONSOLA CIS/CVS 1-3-4 MAZAR-MOLINO	[10]	[10]	[10]
[MID_CCC_HPA_MAZ] CONSOLA CCC MAZAR-MOLINO	[10]	[10]	[10]
[MID_CONTROCAD_HPA_MAZ] CONTROCAD SERVER MAZAR-MOLINO	[10]	[10]	[10]
[MID_C10_HPA_MAZ] CONSOLA C10	[10]	[10]	[10]
[PC_HPA_MAZ] SCAD-AROCHE-ION-PROTECCIONES-DATOSCM-DATOS	[7]	[7]	[7]
[DATA_VIBRACIONES_HPA_MAZ] VIBRACIONES_SERVER	[9]	[9]	[9]
[COM] Comunicaciones			
[COM_RED S8000] RED S8000-1/2	[10]	[10]	[10]
[COM_RED F8000-1/2] RED F8000-1/2	[10]	[10]	[10]
[COM_RED OFFICE] RED OFFICE	[8]	[8]	[8]
[COM_LAN] RED LAN	[7]	[7]	[7]
[PABX_TELEF_HPA_MAZ] CENTRAL TELEFONICA MAZAR	[3]	[3]	[3]
[Media] Soportes de información			
[DVD_HPA_MAZ] INSTALADORES SCADA ALSPA P320	[7]	[7]	[5]
[D] Datos			
[FILES_HISTORIAN] BASE DE DATOS	[10]	[10]	[10]
[FILES_SCAD] BASE DE DATOS SCAD	[7]	[7]	[7]
[FILES_AROCHE] BASE DE DATOS AROCHE	[7]	[7]	[7]
[FILES_VIBRACIONES_HPA_MAZ] ZOOM	[7]	[7]	[7]
[FILES_ARGIS] BASE DE DATOS PROTECCIONES ARGIS	[7]	[7]	[7]
[FILES_DESCARGASPARCIALES_HPA_MAZ] DESCARGASPARCIALES	[7]	[7]	[7]
[FILES_LOGGERNET] BASE DE DATOS LOGGERNET	[7]	[7]	[7]
[FILES_ION] BASE DE DATOS ION	[7]	[7]	[7]

Figura 2.17. Valoración de los activos

Fuente: Propia

Elaborado: Alfredo Carpio

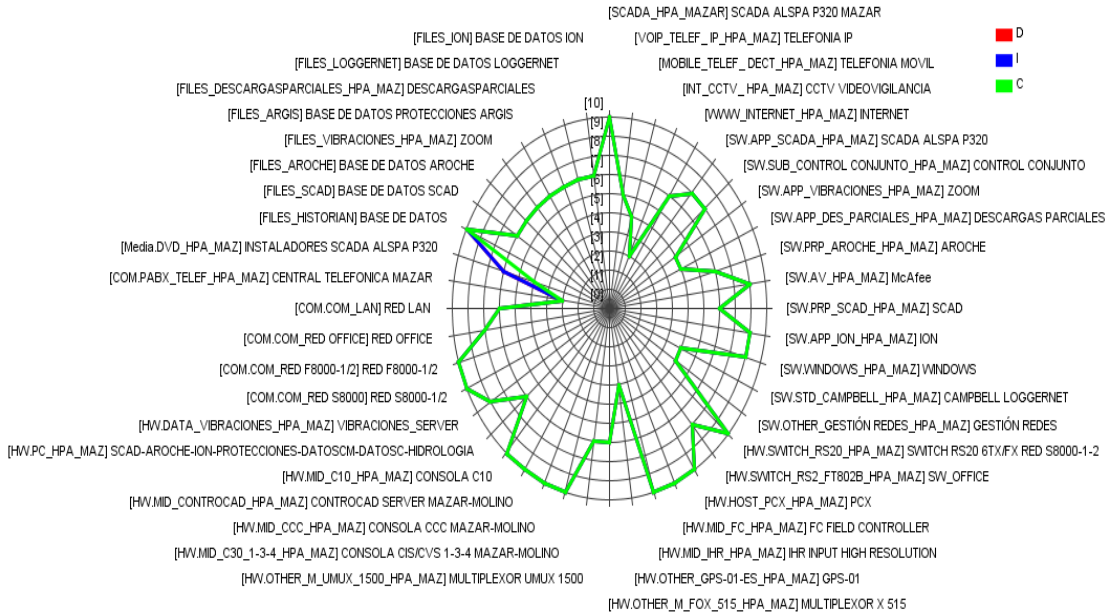


Figura 2.18. Valoración de los activos (tipo araña)

Fuente: Propia

Elaborado: Alfredo Carpio

Con la valoración correspondiente a cada uno de los activos y su relación estrecha con los procesos críticos de la organización se establece la Tabla 9 donde se presenta los activos de información que tienen un valor de 10 alto índice de criticidad.

Tabla 9. Activos críticos de proceso de entrega de energía

NOMBRE	VALORACIÓN
SCADA ALSPA P320 MAZAR	10
SWITCH_RS20	10
PCX	10
FC FIELD CONTROLLER	10
HR INPUT HIGH RESOLUTION	10
CIS/CVS 1-3-4 MAZAR-MOLINO	10
CONSOLA CCC MAZAR-MOLINO	10
CONTROCAD SERVER MAZAR-MOLINO	10
CONSOLA C10	10
RED S8000-1/2	10
RED F8000-1/2	10
BASE DE DATOS	10

Fuente: Propia

Elaborado: Alfredo Carpio

Tabla 10. MTPoD, RTO y RPO

NOMBRE	MTPoD	RTO	RPO
SCADA ALSPA P320 MAZAR	4 Horas 25 minutos	3 Horas 30 minutos	24 horas
SWITCH_RS20	2 Horas	1Hora 30 minutos	24 horas
PCX	4 Horas 25 minutos	3 Horas 30 minutos	24 horas
FC FIELD CONTROLLER			24 horas
HR INPUT HIGH RESOLUTION			24 horas
CIS/CVS 1-3-4 MAZAR-MOLINO	4 Horas 25 minutos	3 Horas 30 minutos	24 horas
CONSOLA CCC MAZAR-MOLINO			24 horas
CONTROCAD SERVER MAZAR-MOLINO			24 horas

CONSOLA C10			24 horas
RED S8000-1/2	4 Horas 25 minutos	3 Horas 30 minutos	24 horas
RED F8000-1/2			24 horas
BASE DE DATOS	4 Horas 25 minutos	3 Horas 30 minutos	24 horas

Fuente: Propia

Elaborado: Alfredo Carpio

2.5 Identificar los eventos o cadenas de eventos que puedan ocasionar interrupciones en los procesos críticos del negocio

Luego de las entrevistas con los dueños de los procesos y los técnicos que laboran y que están inmersos en el adecuado funcionamiento de los mismos, se establecen las siguientes amenazas como posibles desencadenadores de interrupciones en el proceso de Operación Central Mazar y sus subprocesos correspondientes, para esto se dividen en 4 grupos principales (Figura 2.19): [N]Desastres naturales, [I]De origen Industrial, [E]Errores y fallos no intencionados y Ataques deliberados, en el Anexo B se presentan las diferentes amenazas detectadas para cada activo en cada uno de los 4 grupos mencionados anteriormente.

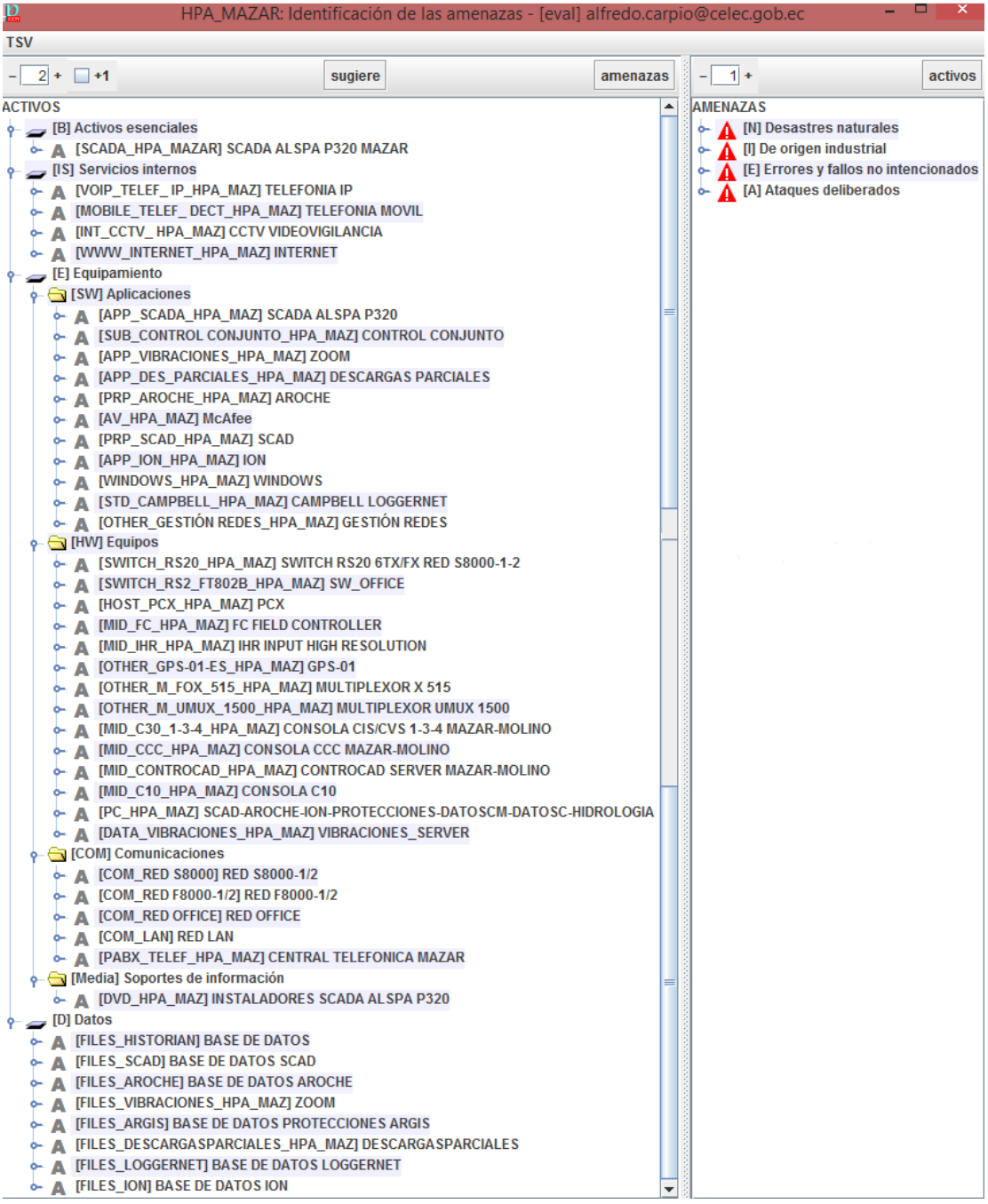


Figura 2.19. Identificación de Amenazas

Fuente: Propia

Elaborado: Alfredo Carpio

2.6 Analizar y evaluar la probabilidad de ocurrencia y el impacto que puedan tener las interrupciones causadas por incidentes de seguridad de la información

Para la valoración de las amenazas se han tomado en cuenta una escala cualitativa, es así que para la probabilidad de que ocurra una determinada amenaza se tiene una escala desde cero a casi seguro (Figura 2.20).

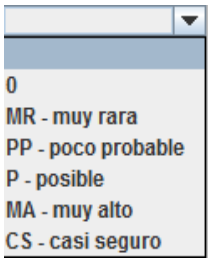


Figura 2.20. Valoración de Probabilidad de Amenazas

Fuente: Propia

Elaborado: Alfredo Carpio

Para la valoración del impacto que causase si se materializa una amenaza sobre el activo de información la escala de valoración va desde cero a Total (Figura 2.21).

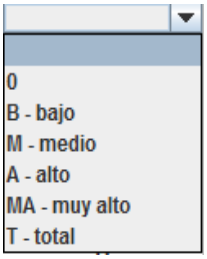
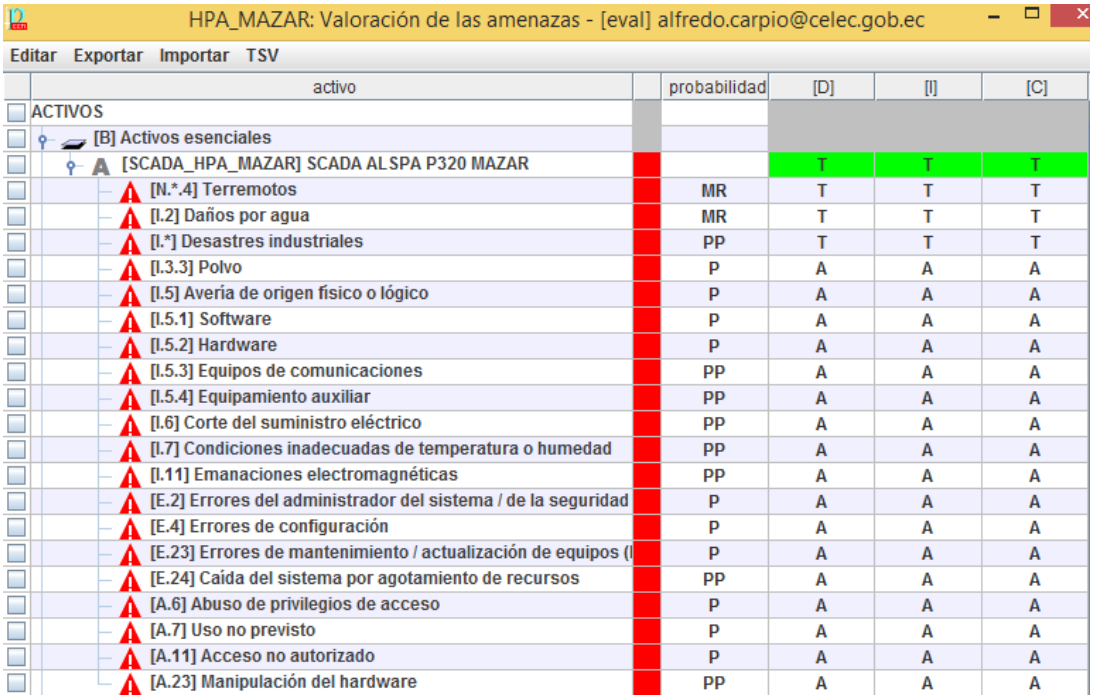


Figura 2.21. Valoración de Impacto de Amenazas

Fuente: Propia

Elaborado: Alfredo Carpio

Tomando en cuenta estos criterios se ha procedido a valorar tanto la probabilidad y el impacto a cada uno de los activos de información, por ejemplo la valoración a los activos esenciales (Figura 2.22). El resto de activos valorados lo vemos en el Anexo C.



activo	probabilidad	[D]	[I]	[C]
ACTIVOS				
[B] Activos esenciales				
[SCADA_HPA_MAZAR] SCADA ALSPA P320 MAZAR		T	T	T
[N.*.4] Terremotos	MR	T	T	T
[I.2] Daños por agua	MR	T	T	T
[I.*] Desastres industriales	PP	T	T	T
[I.3.3] Polvo	P	A	A	A
[I.5] Avería de origen físico o lógico	P	A	A	A
[I.5.1] Software	P	A	A	A
[I.5.2] Hardware	P	A	A	A
[I.5.3] Equipos de comunicaciones	PP	A	A	A
[I.5.4] Equipamiento auxiliar	PP	A	A	A
[I.6] Corte del suministro eléctrico	PP	A	A	A
[I.7] Condiciones inadecuadas de temperatura o humedad	PP	A	A	A
[I.11] Emanaciones electromagnéticas	PP	A	A	A
[E.2] Errores del administrador del sistema / de la seguridad	P	A	A	A
[E.4] Errores de configuración	P	A	A	A
[E.23] Errores de mantenimiento / actualización de equipos (I	P	A	A	A
[E.24] Caída del sistema por agotamiento de recursos	PP	A	A	A
[A.6] Abuso de privilegios de acceso	P	A	A	A
[A.7] Uso no previsto	P	A	A	A
[A.11] Acceso no autorizado	P	A	A	A
[A.23] Manipulación del hardware	PP	A	A	A

Figura 2.22. Valoración de Amenazas de los activos esenciales.

Fuente: Propia

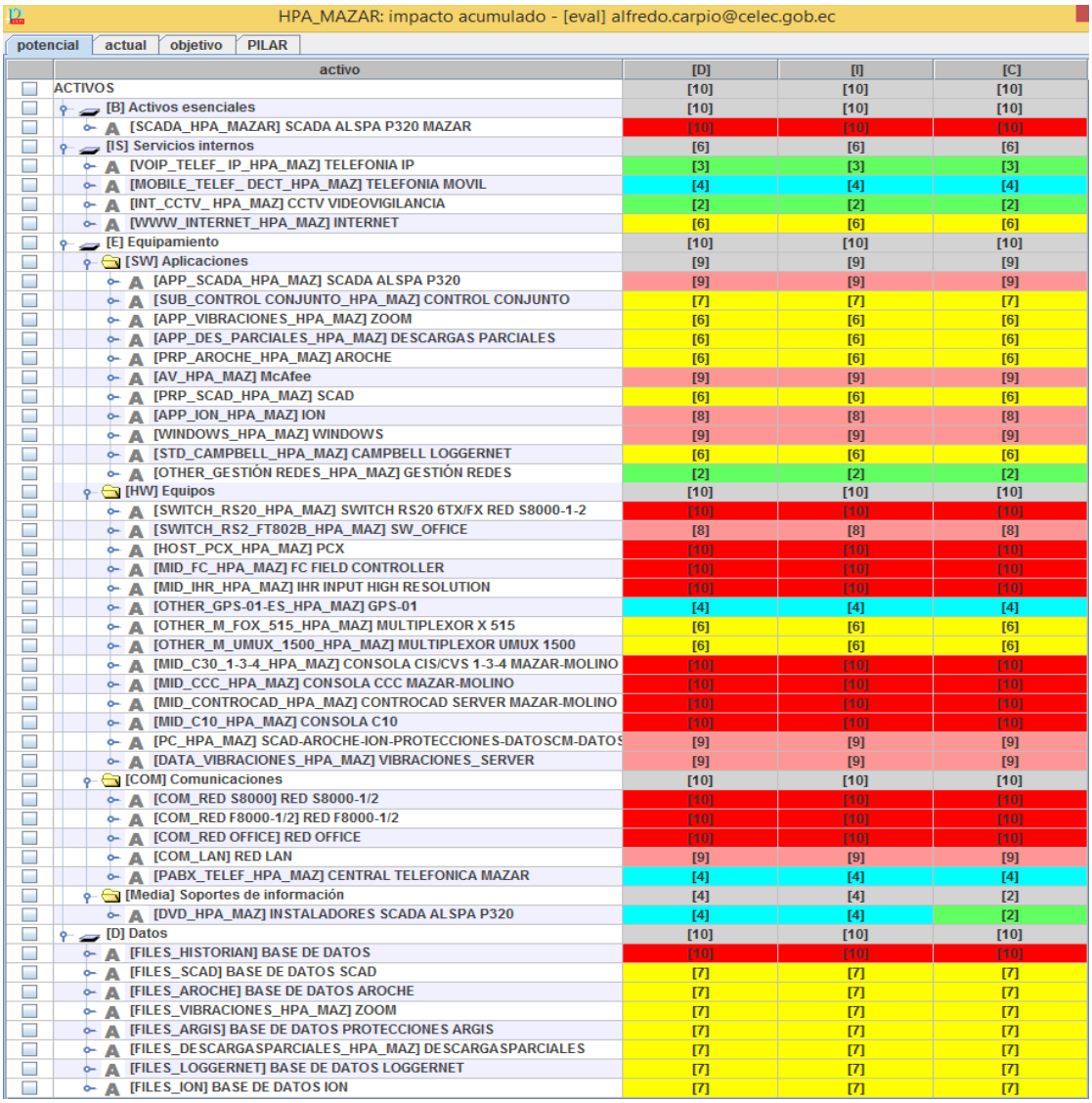
Elaborado: Alfredo Carpio

Un resumen total del Impacto y su representación mediante colores lo podemos apreciar en la Figura 2.23 y Figura 2.24.

Figura 2.23. Valoración de Impacto Acumulado y significado en colores.

Fuente: Propia

Elaborado: Alfredo Carpio



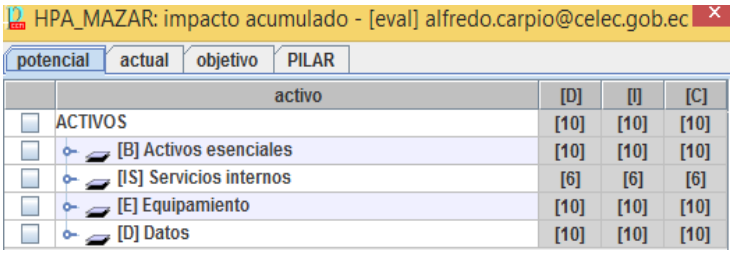
activo	[D]	[I]	[C]
ACTIVOS	[10]	[10]	[10]
[B] Activos esenciales	[10]	[10]	[10]
[SCADA_HPA_MAZAR] SCADA ALSPA P320 MAZAR	[10]	[10]	[10]
[IS] Servicios internos	[6]	[6]	[6]
[VOIP_TELEF_ IP_HPA_MAZ] TELEFONIA IP	[3]	[3]	[3]
[MOBILE_TELEF_ DECT_HPA_MAZ] TELEFONIA MOVIL	[4]	[4]	[4]
[INT_CCTV_ HPA_MAZ] CCTV VIDEOVIGILANCIA	[2]	[2]	[2]
[WWW_INTERNET_HPA_MAZ] INTERNET	[6]	[6]	[6]
[E] Equipamiento	[10]	[10]	[10]
[SW] Aplicaciones	[9]	[9]	[9]
[APP_SCADA_HPA_MAZ] SCADA ALSPA P320	[9]	[9]	[9]
[SUB_CONTROL CONJUNTO_HPA_MAZ] CONTROL CONJUNTO	[7]	[7]	[7]
[APP_VIBRACIONES_HPA_MAZ] ZOOM	[6]	[6]	[6]
[APP_DES_PARCIALES_HPA_MAZ] DESCARGAS PARCIALES	[6]	[6]	[6]
[PRP_AROCHE_HPA_MAZ] AROCHE	[6]	[6]	[6]
[AV_HPA_MAZ] McAfee	[9]	[9]	[9]
[PRP_SCAD_HPA_MAZ] SCAD	[6]	[6]	[6]
[APP_ION_HPA_MAZ] ION	[8]	[8]	[8]
[WINDOWS_HPA_MAZ] WINDOWS	[9]	[9]	[9]
[STD_CAMPBELL_HPA_MAZ] CAMPBELL LOGGERNET	[6]	[6]	[6]
[OTHER_GESTIÓN REDES_HPA_MAZ] GESTIÓN REDES	[2]	[2]	[2]
[HW] Equipos	[10]	[10]	[10]
[SWITCH_RS20_HPA_MAZ] SWITCH RS20 6TX/FX RED S8000-1-2	[10]	[10]	[10]
[SWITCH_RS2_FT802B_HPA_MAZ] SW_OFFICE	[8]	[8]	[8]
[HOST_PCX_HPA_MAZ] PCX	[10]	[10]	[10]
[MID_FC_HPA_MAZ] FC FIELD CONTROLLER	[10]	[10]	[10]
[MID_IHR_HPA_MAZ] IHR INPUT HIGH RESOLUTION	[10]	[10]	[10]
[OTHER_GPS-01-ES_HPA_MAZ] GPS-01	[4]	[4]	[4]
[OTHER_M_FOX_515_HPA_MAZ] MULTIPLEXOR X 515	[6]	[6]	[6]
[OTHER_M_UMUX_1500_HPA_MAZ] MULTIPLEXOR UMUX 1500	[6]	[6]	[6]
[MID_C30_1-3-4_HPA_MAZ] CONSOLA CIS/CVS 1-3-4 MAZAR-MOLINO	[10]	[10]	[10]
[MID_CCC_HPA_MAZ] CONSOLA CCC MAZAR-MOLINO	[10]	[10]	[10]
[MID_CONTROCAD_HPA_MAZ] CONTROCAD SERVER MAZAR-MOLINO	[10]	[10]	[10]
[MID_C10_HPA_MAZ] CONSOLA C10	[10]	[10]	[10]
[PC_HPA_MAZ] SCAD-AROCHE-ION-PROTECCIONES-DATOSCM-DATOS	[9]	[9]	[9]
[DATA_VIBRACIONES_HPA_MAZ] VIBRACIONES_SERVER	[9]	[9]	[9]
[COM] Comunicaciones	[10]	[10]	[10]
[COM_RED S8000] RED S8000-1/2	[10]	[10]	[10]
[COM_RED F8000-1/2] RED F8000-1/2	[10]	[10]	[10]
[COM_RED OFFICE] RED OFFICE	[10]	[10]	[10]
[COM_LAN] RED LAN	[9]	[9]	[9]
[PABX_TELEF_HPA_MAZ] CENTRAL TELEFONICA MAZAR	[4]	[4]	[4]
[Media] Soportes de información	[4]	[4]	[2]
[DVD_HPA_MAZ] INSTALADORES SCADA ALSPA P320	[4]	[4]	[2]
[D] Datos	[10]	[10]	[10]
[FILES_HISTORIAN] BASE DE DATOS	[10]	[10]	[10]
[FILES_SCAD] BASE DE DATOS SCAD	[7]	[7]	[7]
[FILES_AROCHE] BASE DE DATOS AROCHE	[7]	[7]	[7]
[FILES_VIBRACIONES_HPA_MAZ] ZOOM	[7]	[7]	[7]
[FILES_ARGIS] BASE DE DATOS PROTECCIONES ARGIS	[7]	[7]	[7]
[FILES_DESCARGASPARCIALES_HPA_MAZ] DESCARGASPARCIALES	[7]	[7]	[7]
[FILES_LOGGERNET] BASE DE DATOS LOGGERNET	[7]	[7]	[7]
[FILES_ION] BASE DE DATOS ION	[7]	[7]	[7]

Figura 2.24. Resultado de Impacto Acumulado

Fuente: Propia

Elaborado: Alfredo Carpio

En la siguiente Figura 2.25 se pude observar el impacto acumulado por las cuatro capas de activos que se habían definido previamente, además se presenta una representación gráfica tipo araña del impacto acumulado por activo (Figura 2.26).



activo	[D]	[I]	[C]
ACTIVOS	[10]	[10]	[10]
[B] Activos esenciales	[10]	[10]	[10]
[IS] Servicios internos	[6]	[6]	[6]
[E] Equipamiento	[10]	[10]	[10]
[D] Datos	[10]	[10]	[10]

Figura 2.25. Impacto Acumulado por capas.

Fuente: Propia

Elaborado: Alfredo Carpio

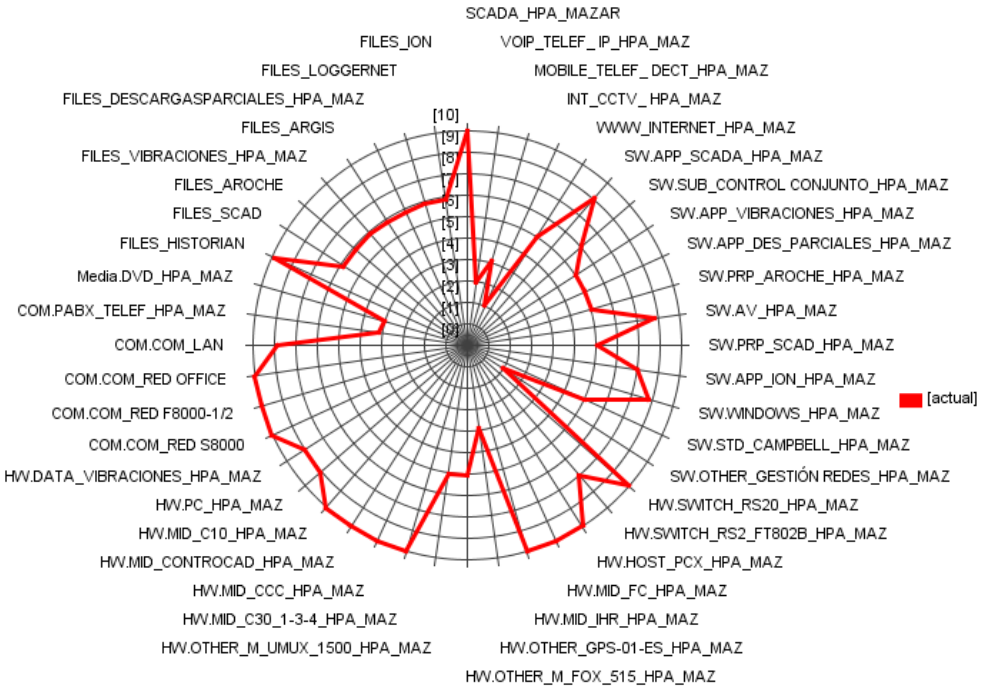


Figura 2.26. Impacto acumulado por activo (tipo araña).

Fuente: Propia

Elaborado: Alfredo Carpio

Resumen Total de Riesgo

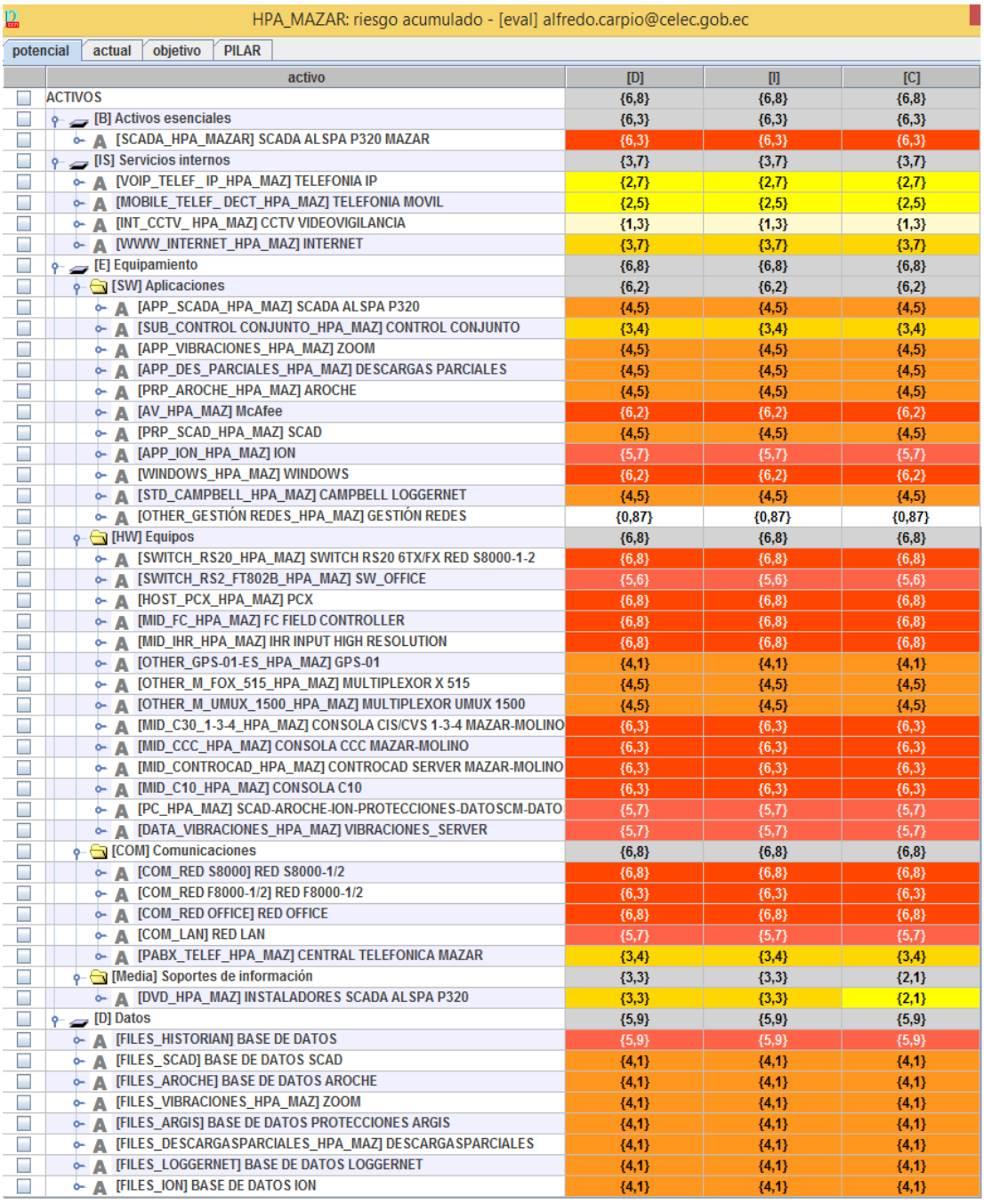
Los niveles de criticidad para el riesgo son representados mediante colores (Figura 2.27) en una escala cualitativa que va desde cero-despreciable hasta nueve-catástrofe.

Figura 2.27. Niveles de criticidad.

Fuente: Propia

Elaborado: Alfredo Carpio

Igualmente para cada activo de información se establecen los riesgos acumulados en las tres dimensiones de Disponibilidad, Confidencialidad e Integridad, tal cual se refleja en la Figura 2.28.



HPA_MAZAR: riesgo acumulado - [eval] alfredo.carpio@celec.gob.ec

potencial | actual | objetivo | PILAR

activo	[D]	[I]	[C]
ACTIVOS	{6,8}	{6,8}	{6,8}
[B] Activos esenciales	{6,3}	{6,3}	{6,3}
[SCADA_HPA_MAZAR] SCADA ALSPA P320 MAZAR	{6,3}	{6,3}	{6,3}
[IS] Servicios internos	{3,7}	{3,7}	{3,7}
[VOIP_TELEF_ IP_HPA_MAZ] TELEFONIA IP	{2,7}	{2,7}	{2,7}
[MOBILE_TELEF_ DECT_HPA_MAZ] TELEFONIA MOVIL	{2,5}	{2,5}	{2,5}
[INT_CCTV_ HPA_MAZ] CCTV VIDEOVIGILANCIA	{1,3}	{1,3}	{1,3}
[WWW_INTERNET_HPA_MAZ] INTERNET	{3,7}	{3,7}	{3,7}
[E] Equipamiento	{6,8}	{6,8}	{6,8}
[SW] Aplicaciones	{6,2}	{6,2}	{6,2}
[APP_SCADA_HPA_MAZ] SCADA ALSPA P320	{4,5}	{4,5}	{4,5}
[SUB_CONTROL CONJUNTO_HPA_MAZ] CONTROL CONJUNTO	{3,4}	{3,4}	{3,4}
[APP_VIBRACIONES_HPA_MAZ] ZOOM	{4,5}	{4,5}	{4,5}
[APP_DES_PARCIALES_HPA_MAZ] DESCARGAS PARCIALES	{4,5}	{4,5}	{4,5}
[PRP_AROCHE_HPA_MAZ] AROCHE	{4,5}	{4,5}	{4,5}
[AV_HPA_MAZ] McAfee	{6,2}	{6,2}	{6,2}
[PRP_SCAD_HPA_MAZ] SCAD	{4,5}	{4,5}	{4,5}
[APP_ION_HPA_MAZ] ION	{5,7}	{5,7}	{5,7}
[WINDOWS_HPA_MAZ] WINDOWS	{6,2}	{6,2}	{6,2}
[STD_CAMPBELL_HPA_MAZ] CAMPBELL LOGGERNET	{4,5}	{4,5}	{4,5}
[OTHER_GESTIÓN REDES_HPA_MAZ] GESTIÓN REDES	{0,87}	{0,87}	{0,87}
[HW] Equipos	{6,8}	{6,8}	{6,8}
[SWITCH_RS20_HPA_MAZ] SWITCH RS20 6TX/FX RED S8000-1-2	{6,8}	{6,8}	{6,8}
[SWITCH_RS2_FT802B_HPA_MAZ] SW_OFFICE	{5,6}	{5,6}	{5,6}
[HOST_PCX_HPA_MAZ] PCX	{6,8}	{6,8}	{6,8}
[MID_FC_HPA_MAZ] FC FIELD CONTROLLER	{6,8}	{6,8}	{6,8}
[MID_IHR_HPA_MAZ] IHR INPUT HIGH RESOLUTION	{6,8}	{6,8}	{6,8}
[OTHER_GPS-01-ES_HPA_MAZ] GPS-01	{4,1}	{4,1}	{4,1}
[OTHER_M_FOX_515_HPA_MAZ] MULTIPLEXOR X 515	{4,5}	{4,5}	{4,5}
[OTHER_M_UMUX_1500_HPA_MAZ] MULTIPLEXOR UMUX 1500	{4,5}	{4,5}	{4,5}
[MID_C30_1-3-4_HPA_MAZ] CONSOLA CIS/CVS 1-3-4 MAZAR-MOLINO	{6,3}	{6,3}	{6,3}
[MID_CCC_HPA_MAZ] CONSOLA CCC MAZAR-MOLINO	{6,3}	{6,3}	{6,3}
[MID_CONTROCAD_HPA_MAZ] CONTROCAD SERVER MAZAR-MOLINO	{6,3}	{6,3}	{6,3}
[MID_C10_HPA_MAZ] CONSOLA C10	{6,3}	{6,3}	{6,3}
[PC_HPA_MAZ] SCAD-AROCHE-ION-PROTECCIONES-DATOSCM-DATO	{5,7}	{5,7}	{5,7}
[DATA_VIBRACIONES_HPA_MAZ] VIBRACIONES_SERVER	{5,7}	{5,7}	{5,7}
[COM] Comunicaciones	{6,8}	{6,8}	{6,8}
[COM_RED S8000] RED S8000-1/2	{6,8}	{6,8}	{6,8}
[COM_RED F8000-1/2] RED F8000-1/2	{6,3}	{6,3}	{6,3}
[COM_RED OFFICE] RED OFFICE	{6,8}	{6,8}	{6,8}
[COM_LAN] RED LAN	{5,7}	{5,7}	{5,7}
[PABX_TELEF_HPA_MAZ] CENTRAL TELEFONICA MAZAR	{3,4}	{3,4}	{3,4}
[Media] Soportes de información	{3,3}	{3,3}	{2,1}
[DVD_HPA_MAZ] INSTALADORES SCADA ALSPA P320	{3,3}	{3,3}	{2,1}
[D] Datos	{5,9}	{5,9}	{5,9}
[FILES_HISTORIAN] BASE DE DATOS	{5,9}	{5,9}	{5,9}
[FILES_SCAD] BASE DE DATOS SCAD	{4,1}	{4,1}	{4,1}
[FILES_AROCHE] BASE DE DATOS AROCHE	{4,1}	{4,1}	{4,1}
[FILES_VIBRACIONES_HPA_MAZ] ZOOM	{4,1}	{4,1}	{4,1}
[FILES_ARGIS] BASE DE DATOS PROTECCIONES ARGIS	{4,1}	{4,1}	{4,1}
[FILES_DESCARGASPARCIALES_HPA_MAZ] DESCARGASPARCIALES	{4,1}	{4,1}	{4,1}
[FILES_LOGGERNET] BASE DE DATOS LOGGERNET	{4,1}	{4,1}	{4,1}
[FILES_ION] BASE DE DATOS ION	{4,1}	{4,1}	{4,1}

Figura 2.28. Riesgo Acumulado calculado

Fuente: Propia

Elaborado: Alfredo Carpio

En la siguiente Figura 2.29 se pude observar el riesgo acumulado por las cuatro capas de activos que se habían definido previamente, además se presenta una representación gráfica tipo araña del riesgo acumulado por activo (Figura 2.30).

HPA_MAZAR: riesgo acumulado - [eval] alfredo.carpio@celec.gob.ec

potencial | actual | objetivo | PILAR

activo	[D]	[I]	[C]
ACTIVOS	{6,8}	{6,8}	{6,8}
[B] Activos esenciales	{6,3}	{6,3}	{6,3}
[IS] Servicios internos	{3,7}	{3,7}	{3,7}
[E] Equipamiento	{6,8}	{6,8}	{6,8}
[D] Datos	{5,9}	{5,9}	{5,9}

Figura 2.29. Riesgo acumulado por capas.

Fuente: Propia

Elaborado: Alfredo Carpio

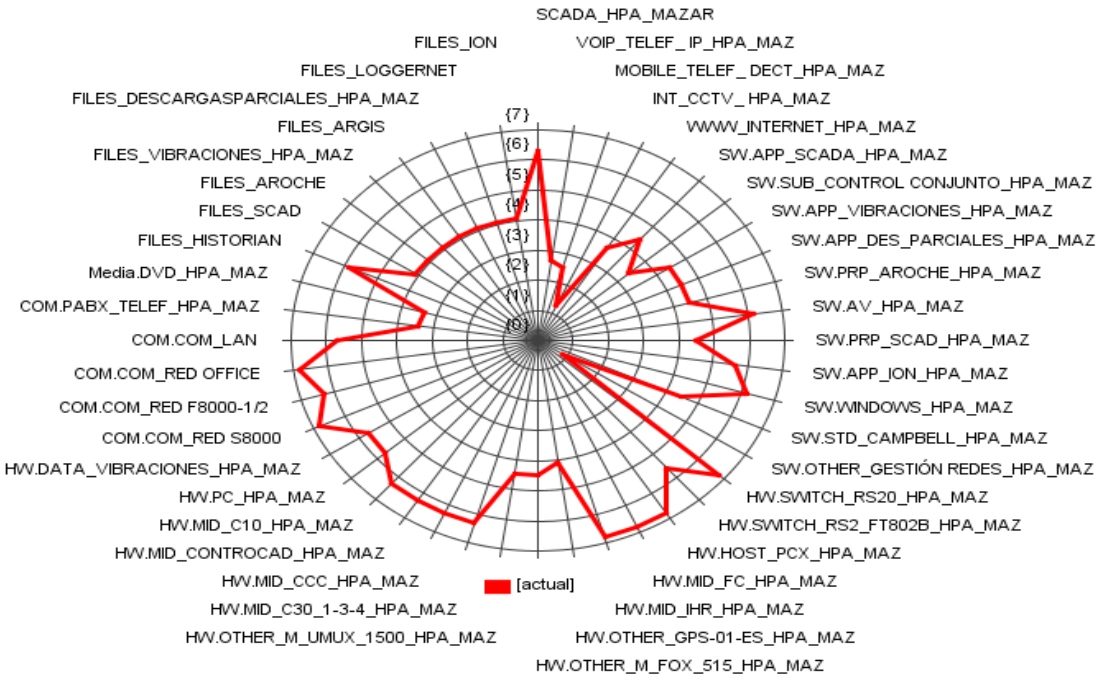


Figura 2.30. Riesgo Acumulado por activo

Fuente: Propia

Elaborado: Alfredo Carpio

Dependencias entre activos de información

Utilizando la herramienta PILAR se establece las dependencias de los activos de información respectivos (Figura 2.31), tomando en cuenta que el activo esencial (SCADA) con el cual el proceso de generación de Paute-Mazar se apalanca.

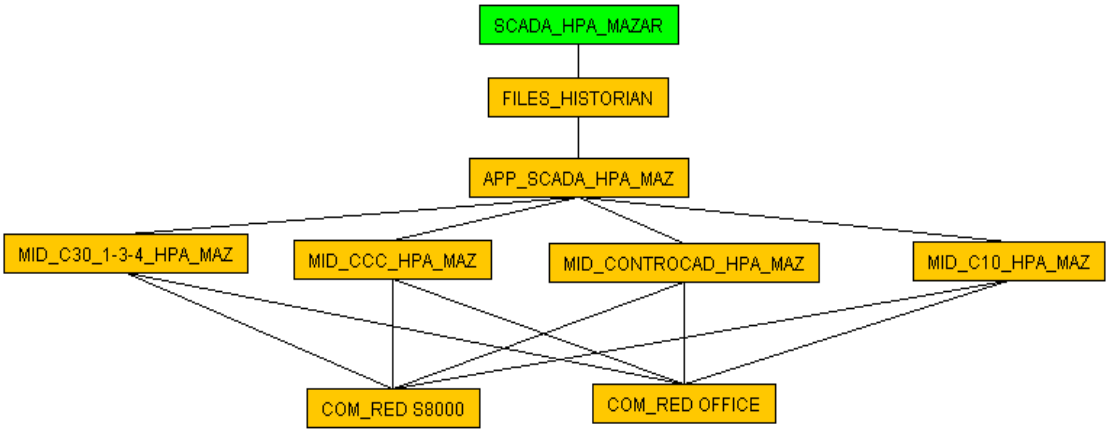


Figura 2.31. Dependencias entre activos.

Fuente: Propia

Elaborado: Alfredo Carpio

CAPÍTULO 3

DESARROLLO DE ESTRATEGIAS DE RECUPERACIÓN TIC.

3.1 Identificar los requerimientos estratégicos para la recuperación de la plataforma de TIC

Tomando en cuenta el análisis de riesgos y los activos comprometidos con ese análisis se puede identificar los requerimientos necesarios para la recuperación de la plataforma de TIC.

Paute-Mazar posee una Casa de Máquinas donde se alojan los generadores eléctricos así como el centro de control de generación desde donde se opera, controla y supervisa la generación de energía eléctrica, en este centro se encuentran los activos de información (Figura3.1) que permiten a la planta de generación

operar normalmente, para el efecto es necesario mencionar los siguientes requerimientos estratégicos:

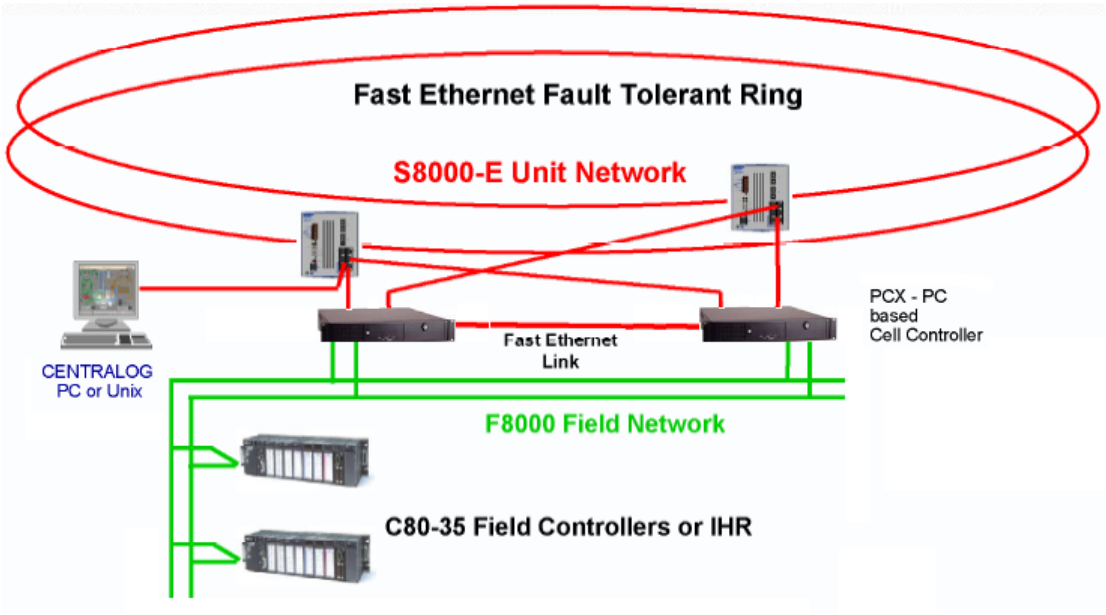


Figura 3.1.SCADA Alspa P320

Fuente: Hidropaute

Elaborado: Alfredo Carpio

1. Establecer y definir el sitio alterno de operación y control.
2. Equipamiento de la RED S8000 1 y 2.
3. Equipamiento de la RED F8000 1 y 2.
4. Equipamiento de CENTRALOG (C10, C30 Mazar).
5. Equipamiento Unidad de Adquisición y Control (UAC1_PCX, UAC2_PCX).
6. Respaldos disponibles para restauración.

7. Formación de Estructura y Equipos de recuperación.

Este equipo de recuperación permitirá monitorear los eventos y de ser el caso recuperar el sistema SCADA de la planta.

3.2 Seleccionar posibles métodos de respaldo y almacenamiento de datos.

Los datos importantes y críticos encontrados en la etapa de análisis de riesgos son los que se recaban en todo el proceso de generación de la planta y que se recolectan en los Historian (bases de datos del sistema Alspa P320), se deben tomar en cuenta ciertos aspectos como:

Las características de los respaldos a priorizar:

- ✓ Confiabilidad (Minimizar las probabilidades de error).
- ✓ Seguridad (Almacenado en un lugar seguro tanto desde el punto de vista de sus requerimientos técnicos como humedad, temperatura, campos magnéticos, como de su seguridad física y lógica).
- ✓ Recuperación (Rápida, probada y eficiente).

Responsables

La responsabilidad de la realización de respaldos será del Analista de Soluciones de Producción, quien vigilará y supervisará que todos los procesos y estándares especificados se desarrollen y cumplan adecuadamente, la operatividad de estos respaldos será delegada al Asistente de Soluciones de Producción.

Información que se incluirá en los respaldos

En cuanto a los respaldos de servidores, la información que incluirá estos respaldos será:

- ✓ Bases de datos de los Historian del sistema SCADA Alspa P320.
- ✓ Base de datos de Control CAD
- ✓ Imagen integra de cada servidor

En cuanto a los respaldos de las configuraciones de las PCX (Cell Controller) de las Unidades de generación U1 y U2 y servicios auxiliares:

- ✓ Imagen integra de configuraciones de PCX

Esquema de respaldos GFS

El esquema de respaldos propuesto es GFS (Grandfather, Father & Son), para el caso de las Bases de datos historian, Base datos CCAD y para las imágenes un respaldo bajo demanda solamente en caso de cambios en configuraciones.

Este esquema de respaldos permitirá mantener copias de la información con la siguiente duración diaria, semanal y mensual de acuerdo a la Tabla 11 y Tabla 12 :

Bases de Datos GFS:

Tabla 11. Esquema respaldos bases de datos

Tipo de	Frecuencia	Tipo de copia	Retención
Grandfather	Mensual	Completa	12 meses
Father	Semanal	Completa	4 semanas
Son	Diaria	Incremental	7 días

Fuente: Propia

Elaborado: Alfredo Carpio

Imágenes servidor: Bajo demanda por cambio de configuración

Tabla 12. Esquema respaldos Imágenes Servidor

Tipo de	Frecuencia	Tipo de copia	Retención
Bajo Demanda	Cada cambio de configuración	Completa	Hasta nuevo cambio de configuración

Fuente: Propia

Elaborado: Alfredo Carpio

Para el caso de las PCX, el esquema de respaldos Tabla 13, se basa en obtener una copia íntegra de las configuraciones cada vez que se realice un cambio de configuración en el equipo PCX.

Imágenes PCX: Bajo demanda por cambio de configuración

Tabla 13. Esquema respaldos Imágenes PCX

Tipo de respaldo	Frecuencia	Tipo de copia	Retención
Bajo Demanda	Cada cambio de configuración	Completa	Hasta nuevo cambio de configuración

Fuente: Propia

Elaborado: Alfredo Carpio

Medios de destino de respaldos

Para la realización de estos respaldos definidos en la Tabla 14 y 15 se deberá definir un servidor específico dedicado para este menester, que cumpla con características de RAID 5 (Redundant Array of Independent or Inexpensive Disks) de capacidad no menor a 1TB. No así para las configuraciones de las PCX que tendrán que respaldarse un una tarjeta Compact Flash de no menos de 128MB de capacidad Tabla 16.

Además se debe obtener una copia de respaldo de bases de datos (diarios) e imágenes (última configuración) y trasladarlos a las oficinas de TIC Arenales, en caso de fallo del servidor se tiene disponible una copia adicional, de igual manera se deberá disponer de una copia (última configuración) de la memoria Compact Flash.

Bases de Datos:

Tabla 14. Medios de respaldos bases de datos.

Tipo de respaldo	Origen de	Medio de destino
Grandfather	Servidores Alspa P320	Disco Duro
Father	Servidores Alspa P320	Disco Duro
Son	Servidores Alspa P320	Disco duro

Fuente: Propia

Elaborado: Alfredo Carpio

Imágenes Servidor:

Tabla 15. Medios de respaldos de imágenes Servidor

Tipo de respaldo	Origen de	Medio de destino
Bajo Demanda	Servidores Alspa P320	Disco duro

Fuente: Propia

Elaborado: Alfredo Carpio

Imágenes PCX:

Tabla 16. Medios de respaldos de imágenes PCX

Tipo de respaldo	Origen de	Medio de destino
Bajo Demanda	PCX	Tarjeta Compact Flash

Fuente: Propia

Elaborado: Alfredo Carpio

Estos respaldos servirán al momento de recuperar la información después de un desastre, sea este parcial o total, además el tener imágenes de disco íntegro del servidor facilitaría y aceleraría el proceso de recuperación ante una falla total de los servidores.

Esto se deberá complementar con una adecuada documentación de configuraciones de cada servidor y PCX, así como características de componentes de software y hardware respectivamente.

Herramientas necesarias

Por mencionar algunas en el mercado dependerá de los requerimientos y costos la decisión de definir una de ellas.

- ✓ Acronis Backup.
- ✓ NetBackup.
- ✓ Backup Exec.
- ✓ Commvault Simpana 10.

Esquema de rotación

El esquema de rotación usado para las Bases de Datos Tablas 17, 18 y 19 será un backup de 7 días por semana, Lunes a Domingo, Lunes a Sábado respaldo incremental y un respaldo completo el día Domingo. Los respaldos se propone realizarlos a las 00H00.

El esquema para las imágenes Tablas 20, 21 y 22 será un respaldo total diario a las 00H00.

Bases de datos:

Tabla 17. Características de respaldo bases de datos

Nombre de esquema	7 días - respaldo incremental semanal, respaldo total en Domingo
Hora de ejecución	00H00
Método de	Incremental
GFS habilitado	Sí
Prefijo de medio	MAZ-BBDD-HIS
Anexar a medio	Sí

Fuente: Propia

Elaborado: Alfredo Carpio

Tabla 18. Retención de respaldo bases de datos Historian

Discos	Retención	Nombre
Diarias	6 días	MAZ_BBDD_HIS__DLY
Semanales	3 semanas	MAZ_BBDD_HIS_WLY
Mensuales	11 meses	MAZ_BBDD_HIS_MLY

Fuente: Propia

Elaborado: Alfredo Carpio

Tabla 19. Método de respaldo bases de datos Historian

Día de la semana	Nombre del medio	Método	Hora de ejecución
Domingo	<Automático>	Full	Predeterminada
Lunes	<Automático>	Incremental	Predeterminada
Martes	<Automático>	Incremental	Predeterminada
Miércoles	<Automático>	Incremental	Predeterminada
Jueves	<Automático>	Incremental	Predeterminada
Viernes	<Automático>	Incremental	Predeterminada
Sábado	<Automático>	Incremental	Predeterminada

Fuente: Propia

Elaborado: Alfredo Carpio

Tabla 20. Método de respaldo bases de datos CCAD

Día de la semana	Nombre del medio	Método	Hora de ejecución
Domingo	<Automático>	Full	Predeterminada
Lunes	<Automático>	Incremental	Predeterminada
Martes	<Automático>	Incremental	Predeterminada
Miércoles	<Automático>	Incremental	Predeterminada
Jueves	<Automático>	Incremental	Predeterminada
Viernes	<Automático>	Incremental	Predeterminada
Sábado	<Automático>	Incremental	Predeterminada

Fuente: Propia

Elaborado: Alfredo Carpio

Imágenes servidor y PCX:

Tabla 21. Características de respaldo imágenes servidor

Nombre de esquema	Bajo Demanda cambio de configuración
Hora de ejecución	00H00
Método de respaldo	Full
GFS habilitado	No
Prefijo de medio	MAZ-IMG-SER
Anexar a medio	Sí

Fuente: Propia

Elaborado: Alfredo Carpio

Tabla 22. Retención de respaldo imágenes servidor y PCX

Discos	Retención	Nombre
Bajo Demanda	Servidores Alspa y PCXP320	MAZ_IMG_SER_DLY MAZ_IMG_PCX_DLY

Fuente: Propia

Elaborado: Alfredo Carpio

3.3 Seleccionar posibles sitios alternos de operación.

Para seleccionar los posibles sitios alternos de operación se han tomado en cuenta la infraestructura actual tecnológica del sistema SCADA, la ubicación geográfica, distancia de movilización e infraestructura física disponible por parte de Hidropaute.

En tal virtud se propone como posibles sitios alternos de operación del sistema SCADA Alspa P320 de la Central Paute-Mazar los siguientes:

- ✓ Las Oficinas de Comunicaciones de Arenales, el cual se ubica aguas abajo de la planta de Generación Paute-Mazar a unos 5km de distancia.
- ✓ El Centro de Control de Generación de la Central Paute-Molino (Guarumales), el cual se ubica aguas abajo la planta de Generación Paute-Mazar a unos 15Km de distancia.

Estos dos posibles sitios alternos Figura 3.2, deberán proveer las características necesarias para poder operar en idénticas condiciones la Central Paute-Mazar, para el efecto se tendrá que definir cuál de ellas es más asequible tanto a nivel técnico-operativo como a nivel económico.

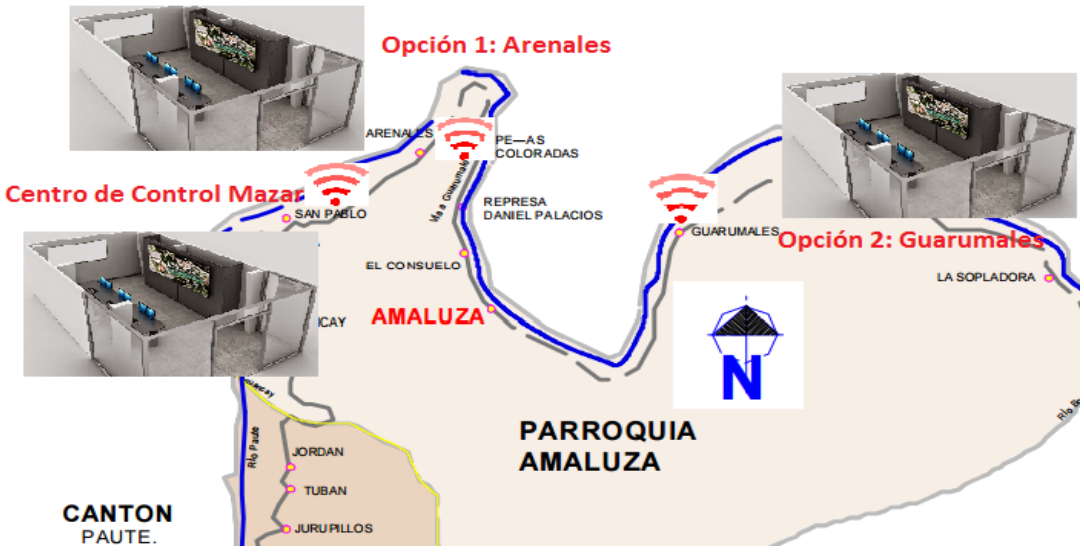


Figura 3.2. Posibles sitios alternos de Operación y Control Paute-Mazar

Fuente: Propia

Elaborado: Alfredo Carpio

3.4 Preparar un análisis costo/beneficio de las estrategias de recuperación.

Para el análisis costo beneficio se toman en cuenta los sitios alternos propuestos en el ítem 3.3:

- ✓ Opción 1: Sitio Alterno Operación Arenales.
- ✓ Opción 2: Sitio Alterno Operación Guarumales.
- ✓ Repuestos de la RED S8000 1 y 2.
- ✓ Repuestos de la RED F8000 1 y 2.
- ✓ Repuestos de C10, C30 Mazar.
- ✓ Repuestos de UAC_1_PCX, UAC_2_PCX y UAC_SA_PCX

Opción 1: Sitio Alterno Operación Arenales

Para el efecto se tiene disponibilidad de espacio físico en las oficinas de TIC Arenales, la cual está junto a la oficina de comunicaciones.

La conectividad entre el centro de control de Paute-Mazar y Arenales es fundamental para que esta opción sea valedera.

En la Figura 3.3 se observa cómo quedaría la conectividad entre los diferentes centros de control de operación (línea negra continua conectividad existente, línea roja entrecortada nueva conectividad):

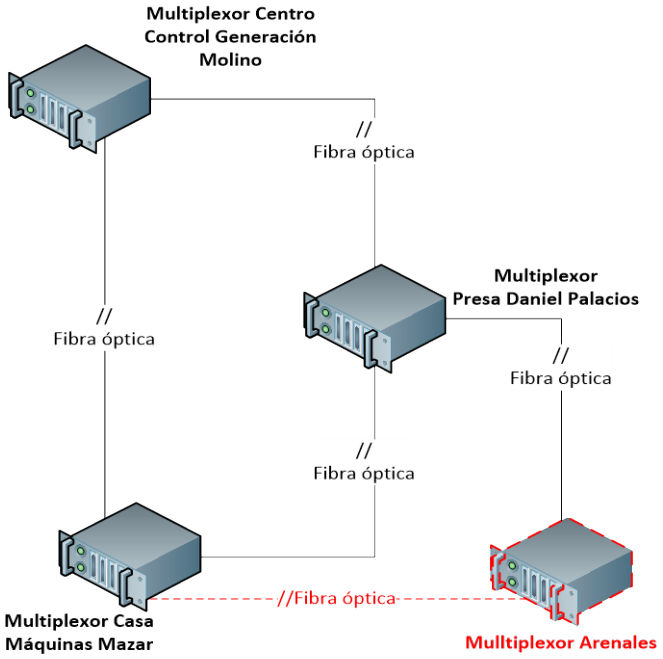


Figura 3.3. Conectividad sitio alterno operación Arenales

Fuente: Propia

Elaborado: Alfredo Carpio

En la Tabla 23 se detalla el requerimiento integral de la opción 1, de tal manera de poder tener el centro de control operativo y listo para su funcionamiento:

Tabla 23. Cuantificación sitio alterno operación Arenales

CANTIDAD	NOMBRE	DESCRIPCIÓN	UNITARIO	TOTAL
1	Multiplexor	Para la transmisión de voz y datos por enlaces de fibra óptica con capacidad de 155Mbit/s, CPU y fuentes de alimentación redundantes, rack, instalación, configuración, puesta en marcha y soporte técnico.	US$44,500.00	US$44,500.00
3	Switch Industrial Administrable	Switch Ethernet, 8 puertas 100BASE-TX, para las redes SE8001, SE8002 y OFFICE	US$2,878.50	US$8,635.50
10	Puntos de red	Conectividad Redes RJ45, CAT-6	US$30.00	US$300.00
1	Impresora B/N	Laser	US$300.00	US$300.00
1	GPS	Para sincronización de tiempo	US$6,000.00	US$6,000.00
5	Km Fibra Óptica	Para interconexión de multiplexor (Recorrido nuevo entre Arenales y Casa Máquinas Mazar)	US$22,000.00	US$110,000.00
1	UPS	Para Servidores 3KVA 120V	US$1,500.00	US$1,500.00
1	SERVIDORES CIS1,CIS2 CCC,CCAD	Estaciones de Operación, Configuracion del sistema e Ingenieria. 1x GX745, 1x Quad Ethernet boards, 2x 21" monitores, 1x extra controladora de video, HHDD 500GB Sistema Operativo: Win XP	US$10,641.86	US$10,641.86
1	SERVIDOR BACKUP	Intel Xeon E5-2620 (2.0GHx/6core), RAID 5, 3 DISCOS 1TB	US$6,000.00	US$6,000.00
1	Mobiliario	Escritorios, Aire Acondicionado, Seguridad Fisica (control de acceso) e Industrial	US$5,000.00	US$5,000.00
1	Configuracion Alspa 320	Técnico de Alspa 320	US$20,000.00	US$20,000.00
			TOTAL	**US$212,877.36**

Fuente: Propia

Elaborado: Alfredo Carpio

El costo total de la estrategia de recuperación del Control y Operación Paute-Mazar desde la opción 1 de Arenales es de aproximadamente de **US$212,877.36** tomando en cuenta su implementación inicial, luego de implementado los costos de la estrategia se basarán en los repuestos necesarios que se requieran para poder solventar las daños físicos y horas hombre de labor de recuperación.

Opción 2: Sitio Alterno Operación Guarumales

Al momento se tiene como una alternativa la operación desde el centro de control de Guarumales esta idea surgió de la posibilidad de poder integrar la operación de las dos centrales Paute-Mazar y Paute-Molino en conjunto, la infraestructura, equipos y conectividad están realizados para el efecto, sin embargo no se la utilizado por diferentes circunstancias logísticas y técnico operativas que debe definirse con la alta dirección de la organización.

Es una alternativa valedera y que viéndola desde una perspectiva económica no tendría gasto adicional alguno para su funcionamiento, excepto de los repuestos necesarios que se

requieran para poder solventar las daños físicos y horas hombre de labor de recuperación.

Repuestos de la RED S8000 1 y 2

Tabla 24. Cuantificación repuestos red S8000

CANTIDAD	NOMBRE	DESCRIPCIÓN	UNITARIO	TOTAL
2	Switch Industrial Administrable	Switch Industrial administrable 4 x 10/100BaseTx, 4x 100BaseFx MM-ST	US$2,878.50	US$5,757.00
2	Switch Industrial Administrable	Switch administrable 16 port Fast-Ethernet: 14 x 10/100 TX-RJ45, 2 x 100BASE-FX MM-SC	US$12,273.00	US$24,546.00
2	Switch Industrial Administrable	Switch Industrial administrable 6xFE TX + 2xFE MM/ST	US$9,187.50	US$18,375.00
			TOTAL	**US$48,678.00**

Fuente: Propia

Elaborado: Alfredo Carpio

Repuestos de la RED F8000 1 y 2

Tabla 25. Cuantificación repuestos red F8000

CANTIDAD	NOMBRE	DESCRIPCIÓN	UNITARIO	TOTAL
2	IR178	Repetidor óptico de redes FIP	US$16,294.00	US$32,588.00
2	RP131	Repetidor óptico de redes FIP	US$16,294.00	US$32,588.00
2	RP132	Repetidor óptico de redes FIP	US$13,375.00	US$26,750.00
			TOTAL	**US$91,926.00**

Fuente: Propia

Elaborado: Alfredo Carpio

Repuestos de C10, C30 Mazar

Tabla 26. Cuantificación repuestos C10 y C30 Mazar

NOMBRE	DESCRIPCIÓN	CANTIDAD	UNITARIO	TOTAL	
CIS01	CPU	1	US$1,050.56	US$1,050.56	
	TARJETA VIDEO x 2 MONITORES	1	US$77.28	US$77.28	
	TARJETA DE RED QUAD ETHERNET PCI CONTROLLER	1	US$492.25	US$492.25	
	MONITOR 2X21	2	US$200.00	US$400.00	
	RAM	2	US$60.00	US$120.00	
	FUENTE DE PODER	1	US$30.00	US$30.00	
	CASE	1	US$50.00	US$50.00	
	MOUSE	1	US$30.00	US$30.00	
	HHDD 250GB	1	US$100.00	US$100.00	**US$2,350.09**
CIS02	CPU	1	US$1,050.56	US$1,050.56	
	TARJETA VIDEO x 2 MONITORES	1	US$77.28	US$77.28	
	TARJETA DE RED QUAD ETHERNET PCI CONTROLLER	1	US$492.25	US$492.25	
	MONITOR 2X21	2	US$200.00	US$400.00	
	RAM	2	US$60.00	US$120.00	
	FUENTE DE PODER	1	US$30.00	US$30.00	
	CASE	1	US$50.00	US$50.00	
	MOUSE	1	US$30.00	US$30.00	
	HHDD 250GB	1	US$100.00	US$100.00	**US$2,350.09**
CCC	CPU	1	US$1,050.56	US$1,050.56	
	TARJETA VIDEO	1	US$50.00	US$50.00	
	TARJETA DE RED 1x serial link card	1	US$350.00	US$350.00	
	MONITOR 1X21	1	US$200.00	US$200.00	
	RAM	2	US$60.00	US$120.00	
	FUENTE DE PODER	1	US$30.00	US$30.00	
	CASE	1	US$50.00	US$50.00	
	MOUSE	1	US$30.00	US$30.00	
	HHDD 250GB	1	US$100.00	US$100.00	**US$1,980.56**
CCAD	CPU	1	US$1,050.56	US$1,050.56	
	TARJETA VIDEO	1	US$50.00	US$50.00	
	TARJETA DE RED 1x serial link card	1	US$350.00	US$350.00	
	MONITOR 1X21	1	US$200.00	US$200.00	
	RAM	2	US$60.00	US$120.00	
	FUENTE DE PODER	1	US$30.00	US$30.00	
	CASE	1	US$50.00	US$50.00	
	MOUSE	1	US$30.00	US$30.00	
	HHDD 250GB	1	US$100.00	US$100.00	**US$1,980.56**
C10	CPU	1	US$1,050.56	US$1,050.56	
	TARJETA VIDEO	1	US$50.00	US$50.00	
	TARJETA DE RED 1x serial link card	1	US$350.00	US$350.00	
	MONITOR 2X21	1	US$200.00	US$200.00	
	RAM	2	US$60.00	US$120.00	
	FUENTE DE PODER	1	US$30.00	US$30.00	
	CASE	1	US$50.00	US$50.00	
	MOUSE	1	US$30.00	US$30.00	
	HHDD 250GB	1	US$100.00	US$100.00	**US$1,980.56**
				TOTAL	**US$10,641.86**

Fuente: Propia

Elaborado: Alfredo Carpio

Repuestos de UAC_1_PCX, UAC_2_PCX

Tabla 27. Cuantificación repuestos UAC_1_PCX, UAC_2_PCX

CANTIDAD	NOMBRE	DESCRIPCIÓN	UNITARIO	TOTAL
2	PCX- PC Based Multi-Function Controller series 5.1 - R1.2 - 6149	PCX controller Series 5.1 - R1.2	US$39,678.00	US$79,356.00
2	C80-35 CPU	C80-35 módulo CPU 360 - Unidad de procesamiento	US$10,782.00	US$21,564.00
2	C80-35 CPU	C80-35 módulo CPU 350 - Unidad de procesamiento	US$6,916.00	US$13,832.00
			TOTAL	**US$114,752.00**

Fuente: Propia

Elaborado: Alfredo Carpio

CAPÍTULO 4

DESARROLLO DEL PLAN DE CONTINGENCIA INFORMÁTICO

4.1 Determinar los requerimientos del plan

Para este Plan de Contingencia Informático de la Central Paute-Mazar es importante contar con una política aprobada por la Alta Gerencia, que sea socializada, además contar con una estructura definida, procedimientos y planes de acción en caso de un incidente que afecte parcialmente o totalmente los activos informáticos críticos del proceso de generación.

En caso de ocurrir una contingencia es importante y esencial que se conozca pormenorizadamente el motivo que la causo y los daños producidos, de esta manera se podrá actuar rápidamente para

restablecer el proceso y la entrega del servicio asociado a la contingencia.

Estos procedimientos deben ser planeados, actualizados y probados periódicamente de tal manera de demostrar fehacientemente su adecuada funcionabilidad en caso de una contingencia, todos estos aspectos se verán detalladamente más adelante.

4.2 Determinar la estructura del plan

La estructura del Plan de Contingencia Informático de la Central Paute-Mazar que se propone, se basa en la realidad actual del orgánico funcional de la Unidad de Negocio Hidropaute, así como la interrelación que se mantiene con entidades internas como externas.

Entidades de coordinación

Para el efecto es necesario mantener las adecuadas relaciones de cooperación y comunicación con entidades internas o externas, las

cuales en su momento pueden colaborar y ayudarnos a solventar cualquier incidente que nos permita volver a brindar los servicios en los tiempos establecidos.

- ✓ Internas
  - o Departamento de Tecnología de la Información y Comunicaciones.
  - o Departamento de Ingeniería de Mantenimiento y Producción.
  - o Departamento de Seguridad Industrial y Salud Laboral.
  - o Departamento de Servicios Generales.

- ✓ Externas
  - o Emergencias (911).
  - o Bomberos Paute (911 - 2250102).
  - o Cruz Roja (131).
  - o Policía Nacional Sevilla de Oro (101 - 2280101).
  - o Aseguradora Equipos Informáticos (Seguros Sucre S.A Telf: 074090328 celular: 0967795023).
  - o Aseguradora contra Incendio y Líneas Aliadas (Rocafuerte Seguros S.A Telf: 074090328 celular: 0967795023).
  - o Ministerio de Salud (171).

- CENACE (Centro Nacional de Control de Energía 022992001).
- Proveedores de Internet y enlace de datos.(Trasnexa 022225099 - Telconet 074134501).
- Proveedores de Hardware y Software. (Coresolutions 072843991).

Organización y conformación del equipo del plan de contingencias

Para la administración, desarrollo, implantación y mantenimiento del Plan de Contingencia Informático de la Central Paute-Mazar, se propone la siguiente estructura la cual está conformada algunos equipos de trabajo los cuales se detallan en el siguiente la Figura 4.1.

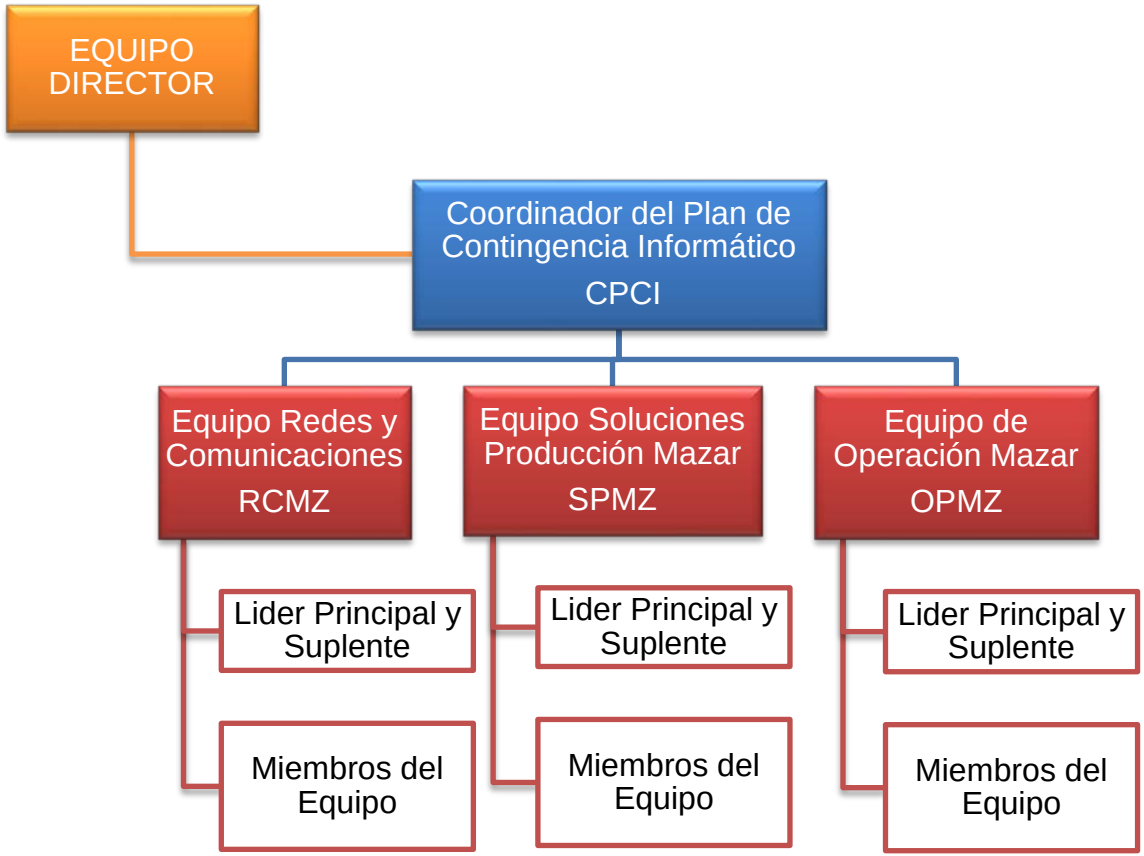


Figura 4.1.Organigrama del Equipo de Plan de Contingencias

Fuente: Propia

Elaborado por: Alfredo Carpio

Equipo Director o Comité de Crisis

El objetivo de este comité es reducir al máximo el riesgo y la incertidumbre en la dirección de la situación. Este Comité debe tomar las decisiones “clave” durante los incidentes, además de hacer de enlace con la dirección de la empresa, manteniéndoles informados de la situación regularmente.

Las principales tareas y responsabilidades de este comité son:

a) Definir todos los lineamientos del Plan de Contingencias de Tecnología de la Información y Comunicaciones.
b) Evaluar y decidir sobre los requerimientos necesarios para el desarrollo, implantación y mantenimiento del plan.
c) Control y seguimiento del desarrollo, implantación y mantenimiento del plan.
d) Evaluar y aprobar la incorporación de convenios, contratos a adquisición de recursos necesarios para el desarrollo, implantación y mantenimiento del plan.
e) Análisis de la situación.
f) Decisión de activar o no el Plan de Contingencia.
g) Iniciar el proceso de notificación a los funcionarios a través de los diferentes responsables.

h) Seguimiento del proceso de recuperación, con relación a los tiempos estimados de recuperación.

i) Determinar de acuerdo a la naturaleza de los daños, donde será el lugar de reunión en caso de pérdida total de las instalaciones.

j) Aportar en la mejora continua del plan de contingencia

En la Tabla 28 se observa la propuesta de conformación de este Equipo Director (* Para el objeto de esta tesis no se muestra toda la información por razones de privacidad).

Tabla 28. Equipo Director o Comité de Crisis

Listado de Integrantes del Comité	
Responsable del Comité	**Nombre: Ing. Tito Torres** **Cargo:** Gerente de CELEC Hidropaute **Teléfono Móvil:** * **Teléfono Casa: *** **Teléfono Oficina:**3700100 ext: *

Miembros del Comité	**LOGISTICA** **Nombre:** Ing. Freddy Vintimilla **Posición:** Subgerente Administrativo **Teléfono Móvil:** * **Teléfono Casa:** * **Teléfono Oficina:**3700100 ext: * **RELACIONES PUBLICAS** **Nombre:** Ing. Tito Torres **Cargo:** Gerente General **Teléfono Móvil: *** **Teléfono Casa:** * **Teléfono Oficina:**3700100 ext: * **EVALUACIÓN DE LA INFRAESTRUCTURA** **Nombre:** Ing. Juan Chávez **Posición:** Subgerente de Producción **Teléfono Móvil:** * **Teléfono Casa:** * **Teléfono Oficina:**3700100 ext: * **Nombre:** Ing. Paúl Cordero

	Posición: Jefe de Central Mazar **Teléfono Móvil:** * **Teléfono Casa:** * **Teléfono Oficina:** 3700140 ext: * **GESTIÓN SOCIO AMBIENTAL** **Nombre:** Ing. David Vázquez **Posición:** Jefe de Gestión Socio Ambiental **Teléfono Móvil: *** **Teléfono Casa:** * **Teléfono Oficina:**3700100 ext: * **GESTIÓN DE SEGURIDAD Y SALUD LABORAL** **Nombre:** Ing. Juan Buñay **Posición:** Jefe de Seguridad y Salud Ocupacional **Teléfono Móvil:** * **Teléfono Casa:** * **Teléfono Oficina:** 3700150 ext: * **MANEJO DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN**

	Nombre: Dr. Javier Zalamea **Posición:** Sub Gerente Gestión Organizacional **Teléfono Móvil:** * **Teléfono Casa:** * **Teléfono Oficina:** 3700100 ext: *

Fuente: Propia

Elaborado: Alfredo Carpio

COORDINADOR DEL PLAN DE CONTINGENCIA INFORMÁTICO

El Coordinador del Plan de Contingencias deberá ser formalmente designado y será el enlace entre el grupo que está ejecutando el plan y el comité de crisis, atreves de este coordinador se transmitirán las decisiones tomadas en torno a las acciones del plan de contingencia, deberá poseer las siguientes capacidades, conocimientos y responsabilidades:

Capacidades / Conocimientos:

a) Liderazgo.

b) Conocimiento de la organización y de los procesos del negocio.
c) Comunicación fluida y clara con otras áreas y departamentos de la organización.
d) Capacidad de gestión de proyectos.

Responsabilidades:

a) Monitorear y asegurar el cumplimiento del plan.
b) Mantener copias del plan actualizadas y encargarse de que se encuentren disponibles para todos los miembros de los diferentes grupos de trabajo del plan.
c) Mantenimiento adecuado de los canales de comunicación entre los diferentes grupos de trabajo del plan.
d) Coordinar las pruebas del plan con el fin de determinar su correcto funcionamiento y entendimiento por parte de los diferentes grupos de trabajo del plan.
e) Proveer los recursos necesarios y notificar las decisiones adoptadas a los funcionarios responsables.
f) Aportar en la mejora continua del plan de contingencia.

En la Tabla 29 se observa la propuesta de coordinador del plan (* Para el objeto de esta tesis no se muestra toda la información por razones de privacidad).

Tabla 29. Equipo Director o Comité de Crisis

Coordinador del Plan de Contingencia Informático (CPCI)	
Coordinador del Plan del Plan Contingencia Informático (CPCI)	**Nombre:** Ing. Marcelo Monteros **Posición:** Jefe de TIC **Teléfono Móvil:** * **Teléfono Casa:** * **Teléfono Oficina:** 3700100 ext: *

Fuente: Propia

Elaborado: Alfredo Carpio

Conformación de equipos de recuperación

Se ha definido tres equipos de recuperación, los cuales estarán conformados por funcionarios que laboran dentro del proceso critico denominado Operación Central Mazar, la información pertinente de los integrantes se encuentran en la Tabla 30.

Equipo de redes y comunicaciones (RCMZ)

Se encarga de las acciones de recuperación de redes y comunicaciones, debiendo reportar al CPCI sobre la interrupción del servicio y progreso de recuperación del mismo.

Responsabilidades:

a) Elaborar y documentar las configuraciones de las redes y comunicaciones de datos.
b) Identificar y determinar el daño de la red y comunicación de datos.
c) Asegurar la disponibilidad y obtener los equipos, partes y piezas a ser remplazados de ser el caso.
d) Coordinar, instalar y configurar el hardware y software requerido para restablecer las comunicaciones.
e) Coordinar con los ISPs para restablecer las comunicaciones.
f) Probar y confirmar el restablecimiento de las comunicaciones.

Equipo de soluciones producción mazar (SPMZ)

Se encarga de las acciones de recuperación de las aplicaciones y equipos críticos, debiendo reportar al CPCI sobre la interrupción del servicio y progreso de recuperación del mismo.

Responsabilidades:

a) Asegurar la disponibilidad y obtener los equipos, partes y piezas a ser remplazados de ser el caso.
b) Asegurar la disponibilidad de los respaldos tanto de las bases de datos, imágenes, configuraciones y aplicaciones necesarios para la recuperación del servicio.
c) Coordinar e instalar el hardware ya sea en el sitio principal o alterno de ser el caso.
d) Coordinar y recuperar datos y aplicaciones en el sitio principal o alterno de ser el caso.
e) Restablecer el ambiente operativo adecuado de operación de las aplicaciones de los servidores.

Equipo de Operación Mazar (OPMZ)

Se encarga de las acciones de restablecimiento de las operaciones de generación de los equipos generadores de electricidad,

debiendo reportar al CPCI sobre la interrupción del servicio y progreso de recuperación del mismo.

Responsabilidades:

a) Reportar e informar de las condiciones (alarmas, bloqueos, etc.) de los equipos informáticos de los generadores de electricidad.
b) Coordinar el restablecimiento de los equipos informáticos y de las operaciones de los generadores de energía eléctrica.

Líderes principales y suplentes de los equipos

Todos y cada uno de los equipos deben tener un Líder y un suplente que lo remplace en caso de ausencia de principal, con suficiente carisma, capacidad de comunicarse, con capacidad de tomar decisiones y trabajo en equipo.

Responsabilidades:

a) Liderar la recuperación de los procesos y sistemas encomendados a su equipo en entornos reales de producción y de pruebas.

b) Participar en la elaboración del análisis de riesgos e impactos de los servicios y procesos encomendados a su equipo.

c) Conocer de manera íntegra los servicios y procesos bajo su responsabilidad.

d) En base a su conocimiento y experiencia aportar en la elaboración y diseño de los procedimientos de recuperación de desastres.

e) Aportar en la mejora continua del plan de contingencia.

f) Servir de enlace entre el equipo de recuperación a su cargo y el CPCI.

g) Interactuar y coordinar con los líderes de los otros equipos recuperación.

h) Mantener información actualizada del estado de recuperación.

i) Gestionar capacitaciones y cursos de actualización al personal de su equipo de recuperación.

.

Ejecutores de equipo

Los miembros del equipo con rol de ejecutores son responsables de las acciones de recuperación y puesta en marcha de los servicios y procesos encargados a su equipo.

Responsabilidades:

a) Ejecutar a tiempo todas y cada una de las actividades planificadas.

b) Comunicar al Líder del equipo todas las necesidades y contratiempos que se presentasen en la recuperación.

c) Aportar en la mejora continua del plan de contingencia.

Tabla 30. Integrantes de Equipos y Roles

Listado de Integrantes de los Equipos		
Equipo Redes y Comunicaciones □RCMZ		
Rol	**Servicios que los soportan**	**Información**
Líder/ Ejecutor	• Red S8001 • Red S8002 • Red F8001 • Red F8002 • Red Corporativa • Comunicaciones	**Nombre:** Ing. Santiago Álvarez **Posición:** Analista de Comunicaciones y Redes **Teléfono Móvil:** * **Teléfono Casa:** * **Teléfono Oficina:** 3700100 ext:*

Ejecutor	• Red S8001 • Red S8002 • Red F8001 • Red F8002 • Red Corporativa • Comunicaciones	**Nombre:** Ing. Andrés Álvarez **Posición:** Asistente de Comunicaciones y Redes **Teléfono Móvil:** * **Teléfono Casa:** * **Teléfono Oficina:** 3700100 ext:*
Ejecutor	• Red S8001 • Red S8002 • Red F8001 • Red F8002 • Red Corporativa • Comunicaciones	**Nombre:** Ing. Diego Tello **Posición:** Asistente de Comunicaciones y Redes **Teléfono Móvil:** * **Teléfono Casa:** * **Teléfono Oficina:** 3700100 ext:*
Equipo Soluciones Producción Mazar□SPMZ		
Rol	**Servicios que los soportan**	**Información**
Líder / Ejecutor	• SCADA ALSPA 320	**Nombre:** Ing. Jaime Matute **Posición:** Analista de Soluciones Producción **Teléfono Móvil:** * **Teléfono Casa:** * **Teléfono Oficina:** 3700100 ext:*

Ejecutor	• SCADA ALSPA 320	**Nombre:** Ing. Lenin Andrade **Posición:** Asistente de Soluciones Producción **Teléfono Móvil:** * **Teléfono Casa:** * **Teléfono Oficina:** 3700100 ext:*
Ejecutor	• SCADA ALSPA 320	**Nombre:** Ing. Geovanny Domínguez **Posición:** Asistente de Soluciones Producción **Teléfono Móvil:** * **Teléfono Casa:** * **Teléfono Oficina:** 3700100 ext:*
Equipo de Operación Mazar□OPMZ		
Rol	**Servicios que los soportan**	**Información**
Líder	• SCADA ALSPA 320 • OPERACIÓN	**Nombre:** Ing. Armando Bernal **Posición:** Jefe de Operación **Teléfono Móvil:** * **Teléfono Casa:** * **Teléfono Oficina:** 3700100 ext:*

Ejecutor	• SCADA ALSPA 320 • OPERACIÓN	**Nombre:** Operador de Turno Sala de Control **Posición:** Operador Sala de Control **Teléfono Móvil:** * **Teléfono Casa:** * **Teléfono Oficina:** 3700100 ext:*
Ejecutor	• SCADA ALSPA 320 • OPERACIÓN	**Nombre:** Operador de turno Casa de Máquinas **Posición:** Operador Casa de Máquinas **Teléfono Móvil:** * **Teléfono Casa:** * **Teléfono Oficina:** 3700100 ext:*

Fuente: Propia

Elaborado: Alfredo Carpio

4.3 Diseñar el plan

En este punto del diseño es importante definir adecuadamente los pasos necesarios que permitan minimizar o evitar la ocurrencia de eventos que paralicen parcial o totalmente los servicios críticos que

componen los Sistemas de Información, los cuales son fundamentales para la organización, se establece un plan de emergencia con la finalidad de restablecer los servicios.

MEDIDAS PREVENTIVAS

SEGURIDAD [N] DESASTRES NATURALES

RIESGO: [N.*.4] Terremotos

RESPONSABLE: Analista de Soluciones de Producción

Medidas Organizativas:

- ✓ Establecer un plan de evacuación del hardware, donde se contemple la prioridad y criticidad de los activos de información que se desean preservar.
- ✓ Etiquetado de los activos de información (preferiblemente con colores) donde se puedan identificar con claridad la prioridad y criticidad de los mismos.
- ✓ Mantener un adecuado registro del personal que está operando en el centro de control.
- ✓ Realizar, mantener y difundir junto con el Jefe de Seguridad y Salud ocupacional el procedimiento pertinente en caso de terremoto que afecte a la planta de generación Paute-Mazar.

Medidas Humanas:

- ✓ Formación del personal para actuar en caso de terremoto que afecte a la planta de generación Paute-Mazar.

SEGURIDAD [I] DE ORIGEN INDUSTRIAL

RIESGO: [I.1] Fuego

RESPONSABLE: Analista de Soluciones de Producción

Medidas Técnicas:

- ✓ El centro de control de operación Mazar, debe contar con un sistema de incendio tipo C de activación manual, debiendo realizarse inspecciones trimestrales de la presión de carga adecuados y deben recargarse mínimo cada 12 meses cuando no han sido utilizados, su remplazo en caso de utilización debe ser en no más de 24 horas. Deben constar con la etiqueta de registro de carga y fecha de vencimiento, así como en buen estado el manómetro de presión que indica el estado del mismo.

- ✓ El centro de control de operación Mazar, debe contar con sensores de humo monitoreado con un sistema que envíe señales tanto auditivas como luminosas en un panel centralizado para el efecto.
- ✓ Se debe capacitar al personal que labora en el centro de operación Mazar sobre el uso y manejo de los extintores mínimo una vez al año.
- ✓ La utilización de equipos de oficina como mesa, escritorios, archivadores, racks y sistemas de bandejas de cable deben ser de material ignifugo (Que protege contra el fuego), evitando daños mayores a los activos de información.
- ✓ Considerar un plan de mantenimiento eléctrico al menos una vez al año, para detectar e impedir posibles cortocircuitos o sobrecargas eléctricas.

Medidas Organizativas:

- ✓ Señalética adecuada basada en políticas de seguridad industrial referentes a la prohibición de fumar en el centro de control de operación Mazar.
- ✓ Mantener un stock de equipos informáticos (repuestos) y tener siempre una ubicación alternativa para poder operar desde otro sitio remoto de ser el caso.

- ✓ Contar con un procedimiento de gestión de respaldos de todos los sistemas críticos de la empresa.
- ✓ Realizar, mantener y difundir el procedimiento en caso de conato de incendio en el centro de operación de Mazar.

Medidas Humanas:

- ✓ Mantener una adecuada formación del personal para actuar en caso de incendio.
- ✓ El personal de la organización debe ser capacitado, para el uso adecuado de los equipos de protección contra incendio (utilización de extintores, mascarillas, tanques de oxígeno personales, etc.).
- ✓ Debe existir un responsable y su respectivo backup del centro de control de generación de Mazar.
- ✓ Debe establecerse claramente los roles y responsabilidades en la gestión de respaldos de información (Bases de datos, configuraciones, imágenes, etc.).

SEGURIDAD [I] DE ORIGEN INDUSTRIAL

RIESGO: [I.2] Daños por agua

RESPONSABLE: Analista de Soluciones de Producción

Medidas Técnicas:

- ✓ El centro de control de operación Mazar, debe contar con sensores inundación de agua por debajo del piso falso, monitoreado con un sistema que dé señales tanto auditivas como luminosas en un panel centralizado para el efecto.
- ✓ Mantener cobertores y plásticos que permitan cubrir los activos de información al menos de manera temporal, en caso de inundación.

Medidas Organizativas:

- ✓ Vigilar el cumplimiento del mantenimiento preventivo, correctivo y programado de las oficinas aledañas al centro de operación Mazar, por donde existen conexiones de cañerías de agua.
- ✓ Contar con un procedimiento en caso de inundación por agua.

SEGURIDAD [I] DE ORIGEN INDUSTRIAL

[I.3] Contaminación medioambiental

RIESGO: [I.3.3] Polvo

RESPONSABLE: Analista de Soluciones de Producción

Medidas Técnicas:

- ✓ Controlar que los servidores y equipos electrónicos estén en una atmósfera libre de polvo, dentro de unos límites estándares de temperatura y humedad relativa (climatización simple: Temperatura dentro de 18°C a 30°C con variaciones inferiores a 5º C por hora, climatización total: Temperatura estable de 21 ± 1°C y una humedad relativa de 50% ± 5%).

Medidas Organizativas:

- ✓ Controlar en donde exista filtros de aire que estos tengan un mantenimiento de limpieza o cambio en caso de deterioro, ya que pueden llegar a bloquearse.
- ✓ Plan de mantenimiento y limpieza que contemple los muros pisos y paredes así como el aspirado del polvo del centro de operación Mazar y comunicaciones.

SEGURIDAD [I] DE ORIGEN INDUSTRIAL

[I.5] Avería de origen Físico o lógico

RIESGO: [I.5.1] Software

RIESGO: [I.5.2] Hardware

RESPONSABLE: Analista de Soluciones de Producción

Medidas Organizativas:

- ✓ Establecer políticas de uso adecuado de los equipos informáticos, que impidan el deterioro de los mismos.
- ✓ Establecer políticas de consumo de alimentos o bebidas al interior del centro de control o área comunicaciones.
- ✓ Plan de mantenimiento de los equipos informáticos mínimo de 6 meses o cada año.
- ✓ Vigilar la existencia y vigencia de las garantías técnicas 1 a 3 años de equipos informáticos contra daño y deterioro.

SEGURIDAD [I] DE ORIGEN INDUSTRIAL

[I.5] Avería de origen Físico o lógico

RIESGO [I.5.3] Equipos de comunicaciones

RESPONSABLE: Asistente de Redes y Comunicaciones

Medidas Técnicas:

- ✓ En las especificaciones de los equipos de comunicaciones, establecer la necesidad de adquirirlos con redundancia es decir, doble fuente de poder, doble ventiladores de enfriamiento, etc.

Medidas Organizativas:

- ✓ Establecer un plan de mantenimiento preventivo al menos una vez al año, para detectar e impedir posibles averías.
- ✓ Mantener un adecuado stock de repuestos que permita minimizar los tiempos de inoperatividad de las comunicaciones.
- ✓ Mantener un adecuado respaldo de las configuraciones de los equipos de comunicaciones.

Medidas Humanas:

- ✓ Mantener una adecuada formación y capacitación del personal de tal manera de poder interactuar con los equipos cuando sea necesario su mantenimiento en caso de remplazo de piezas y partes y restauración de configuraciones de los mismos.

SEGURIDAD [I] DE ORIGEN INDUSTRIAL

[I.6] Corte de suministro eléctrico

RIESGO [I.6.11] Interrupción accidental

RESPONSABLE: Analista de Soluciones de Producción

Medidas Técnicas:

- ✓ Evitar cables de conexión entre equipos y tomas de corriente eléctrica sobre piso falso del centro de operación Mazar, que provoque desconexión accidental de los equipos.
- ✓ Identificación de segregación adecuada de tomas de corriente exclusivas para los activos del centro de control de operación Mazar y tomas de corriente para equipos ajenos al mismo.
- ✓ Verificación de vida útil y funcionamiento adecuados del Suministro de Energía Ininterrumpible (UPS) e Inversores de voltaje que alimentan los activos de información del centro de operación Mazar.

Medidas Organizativas:

- ✓ Los servidores y equipos informáticos deben estar protegidos contra acciones accidentales de golpes y manipulación.
- ✓ Vigilar que se cumpla el plan de mantenimiento preventivo y correctivo del generador de emergencia y UPS de tal manera de garantizar su efectiva operación continua de así requerirlo.
- ✓ Contar con un procedimiento de operación y puesta en marcha del generador de emergencia.

Medidas Humanas:

- ✓ Mantener una adecuada formación y capacitación del personal de tal manera de evitar acciones accidentales sobre los equipos por exceso de confianza.
- ✓ Facilitar capacitación referente a la operación y funcionamiento general del generador de emergencia en casos de prueba y operación en producción.

SEGURIDAD [I] DE ORIGEN INDUSTRIAL

RIESGO: [I.7] Condiciones inadecuadas de temperatura o humedad

RESPONSABLE: Analista de Soluciones de Producción

Medidas Técnicas:

- ✓ Debe existir la menos un sensor de temperatura en el centro de control de operación Mazar, es importante de tal manera de poder actuar inmediatamente en caso de elevaciones importantes de temperaturas.
- ✓ Los servidores deben estar libre de elementos (cobertores, maletines, etc.) que impiden la normal circulación de aire y ventilación de los mismos.
- ✓ Verificar la existencia y buen funcionamiento de los aires acondicionados de confort tanto del principal como del de reserva en caso de falla del primero.

SEGURIDAD: [I] DE ORIGEN INDUSTRIAL

[I.8] Fallo de servicios de comunicaciones

RIESGO: [I.8.11] Interrupción accidental

RESPONSABLE: Asistente de Redes y Comunicaciones

Medidas Técnicas:

- ✓ Evitar cables de conexión entre equipos y tomas de corriente eléctrica sobre piso falso del área de comunicaciones, que provoque desconexión accidental de los equipos.
- ✓ Aplicación de actualizaciones y parches sobre equipos en ambiente controlado.

Medidas Organizativas:

- ✓ Los armarios y racks físicos de acceso a los activos de información del área de comunicaciones deben siempre estar protegidos con cerraduras o llaves que permita el acceso única y exclusivamente al personal autorizado.

Medidas Humanas:

- ✓ Mantener una adecuada formación y capacitación del personal de tal manera de evitar acciones accidentales sobre los equipos y configuraciones por exceso de confianza.

SEGURIDAD: [A] Ataques deliberados

RIESGO: [A.11] Acceso no autorizado

RESPONSABLE: Analista de Soluciones de Producción

Medidas Técnicas:

- ✓ Establecer y vigilar que los permisos de acceso de los usuarios al centro de operación Mazar y las aplicaciones utilizadas sean los adecuados en base al rol del usuario y se cumplan adecuadamente.
- ✓ Los armarios y racks físicos de acceso a los activos de información deben siempre estar protegidos con cerraduras o llaves que permita el acceso única y exclusivamente al personal autorizado.
- ✓ Establecer y verificar la existencia de control físico al centro de operación Mazar ya se mediante tarjetas magnéticas de control o reconocimiento biométrico que facilite la trazabilidad de quien ingresa o sale del centro, así como la

existencia de bitácoras de control para personas que acceden al centro como, visitas, personal de limpieza y mantenimiento.

Medidas Organizativas:

- ✓ Establecer una política de acceso al centro de operación Mazar, donde se pueda obtener una bitácora de registros de quien entra y quién sale, así como mantener una adecuada identificación del personal que labora en el sitio.
- ✓ Elaborar y mantener actualizado un inventario de activos de información.
- ✓ Elaborar y mantener actualizado un registro de los permisos otorgados de acceso de los usuarios a los equipos y aplicaciones del centro de operación Mazar.
- ✓ Establecer una política y procedimientos, donde se establezca como y donde será almacenada los activos de información (documentos físicos y digitales) con los respectivos privilegios y permisos del caso.
- ✓ Vigilar la existencia y vigencia de seguros contra robo, incendio, inundaciones, daño o desastres naturales o industriales que se tienen sobre los activos de información

(hardware y software), e incorporar nuevos activos a ese seguro o excluirlos de ser el caso.

Activación del Plan de Contingencia

Es evidente la necesidad de establecer un canal oficial de activación del plan así como el método para activar o invocar el mismo [12], bajo esa premisa y considerando las responsabilidades del comité de crisis literal *f) Decisión de activar o no el Plan de Contingencia*, recae en el “Responsable del Comité” o su delegado la activación del plan, mismo que será comunicado al CPCI quién activará a los equipos y personal apropiado para realizar las actividades de recuperación establecidas.

En la Figura 4.2 se puede apreciar las 3 fases principales que se desarrollan en el tiempo [13], en cuanto se identifica un incidente o desastre, teniendo en cuenta que estas fases tienen por objetivo que la organización recupere sus procesos y servicios en el menor tiempo posible.

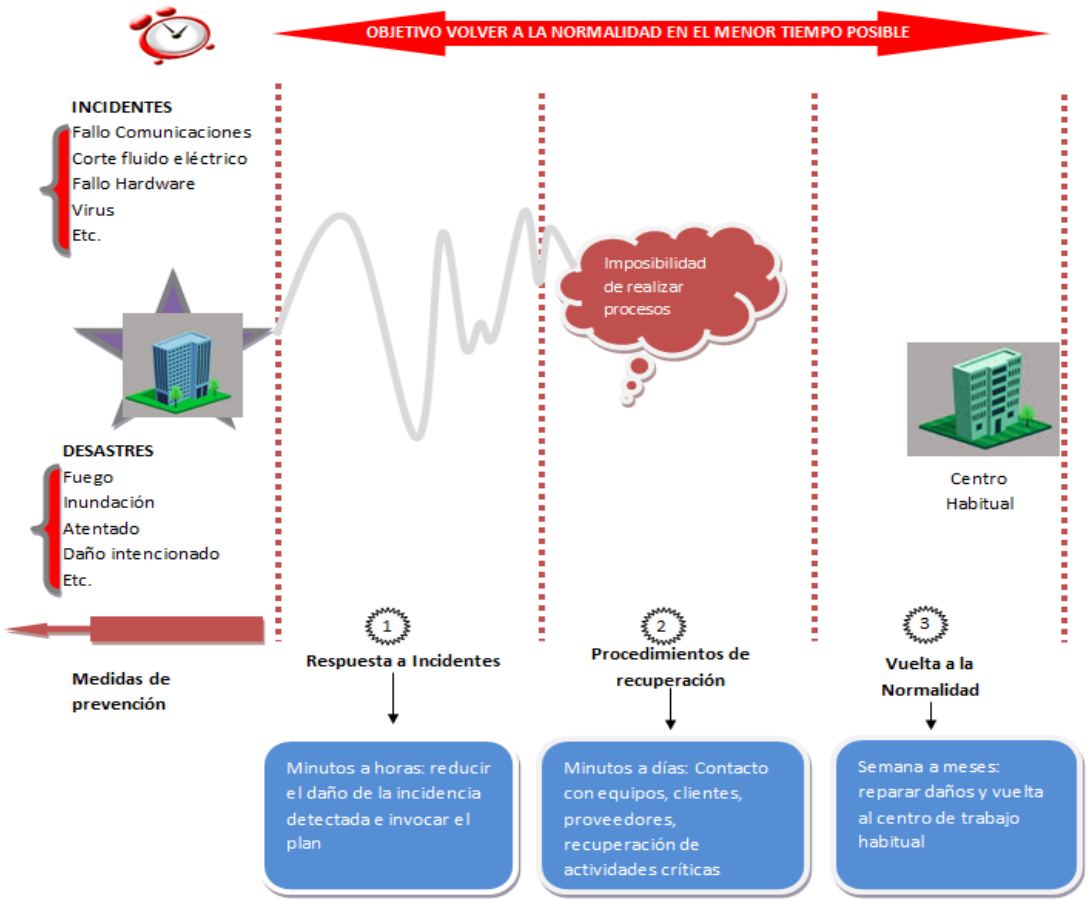


Figura 4.2. Fases de una contingencia en el tiempo

Fuente: (INTECO, 2010)

Elaborado por: Alfredo Carpio

Plan de respuesta a incidentes PRI

Este plan de respuesta a incidentes permitirá que cualquier incidente que se presente en la organización y que interrumpa los

procesos críticos identificados con antelación (Operación Paute-Mazar) tenga una respuesta rápida, ágil que permita:

- ✓ Confirmar el tipo de incidente y su criticidad.
- ✓ Controlar la situación problemática ocasionada por el incidente.
- ✓ Minimizar el impacto que dicho incidente pueda ocasionar.

Secuencias de actuación del PRI

En la Figura 4.3 se visualiza esta secuencia de acciones:

- ✓ Los Operadores de la Central Paute-Mazar reciben notificación (vía telefónica, radio o email) o detectan el incidente de manera visual o sonora, para el efecto recabarán los siguientes datos:
- ✓ Fecha y hora de recepción o detección del incidente.
- ✓ Nombre de la persona que reporta el incidente.
- ✓ Breve descripción del evento.
- ✓ Reporte preliminar de daños.
- ✓ De ser posible número telefónico y ubicación de la persona que reporta el incidente.
- ✓ El Operador de la Central Paute-Mazar comunicará al Jefe de Operación de la Central Paute-Mazar con los datos

recabados anteriormente y agregará la fecha y hora en la que él notifica.

- ✓ El Jefe de Operación de la Central Paute-Mazar analiza el incidente, si afecta la integridad física de las personas, comunica a Jefe de Central Mazar quién activa directamente el Plan de Evacuación del BCP (Business Continuity Plan) de la organización.
- ✓ En su defecto si no afecta la integridad física de las personas el Jefe de Operación de la Central Paute-Mazar analiza la gravedad del incidente estimando los tiempos de interrupción y servicios afectados si no es grave utilizará los procedimientos habituales para corregir el incidente y cerrará el incidente.
- ✓ Si el incidente es grave notificará del mismo al CPCI y a los líderes de los equipos involucrados en el incidente (RCMZ, SPMZ), registrará la fecha y hora de las notificaciones.
- ✓ El CPCI evaluará y verificará la magnitud del incidente, si él no lo puede hacer se contactará con los líderes de los equipos involucrados en el incidente (RCMZ, SPMZ) quienes previamente fueron notificados para que acudan al sitio del incidente, recabará información técnica

especializada de la contingencia y verificación de daños y convocará al comité de crisis.

- ✓ El comité de crisis recibe la información pertinente la analiza y decide activar o no activar el plan.
- ✓ Si decide activar el plan, el responsable del comité comunicará al CPCI y este a su vez comunicará a los equipos involucrados en el incidente (RCMZ, SPMZ, OPMZ) para seleccionar y aplicar los procedimientos de recuperación pertinentes establecidos en el punto 4.4. más adelante. El seguimiento y estado del evento de contingencia lo realizará el CPCI para esto deberá:
  - o Seguir todas las actividades de respuesta y recuperación de los equipos de recuperación.
  - o Documentar el avance de las tareas en orden cronológico, utilizando el Anexo D.
  - o Dar seguimiento y solución a asuntos que pudiesen obstaculizar las labores de los equipos de recuperación.
- ✓ No decide activar el plan, el responsable del comité comunicará al CPCI y este a su vez comunicará al equipo, OPMZ para que utilicen los procedimientos habituales para corregir el incidente y cierre del mismo.

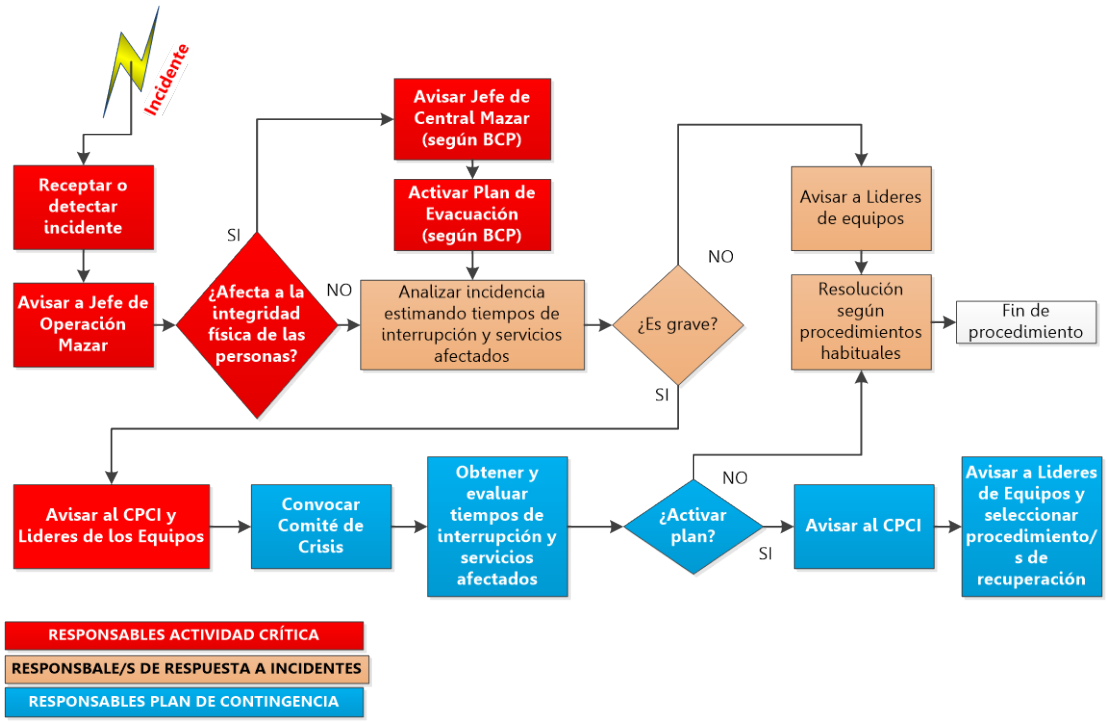


Figura 4.3. Secuencia de actuación del PRI

Fuente: (INTECO, 2010)

Elaborado por: Alfredo Carpio

Procedimientos de recuperación

Estos procedimientos de recuperación (Item 4.4) como se vio pueden ser activados en el plan de respuesta ante incidentes y surgen como consecuencia de la activación del plan, debiendo tener las siguientes secuencia de acciones:

- ✓ Quién y cómo y bajo qué circunstancias se activa el plan.

- ✓ Las personas a ser informadas cuando se activa el plan.
- ✓ Ubicación física de las personas que intervienen en el plan.
- ✓ Que servicios están disponibles.
- ✓ Tiempos y forma de entrega de información a los diferentes estamentos de la organización.

Plan de vuelta a la normalidad

Luego de solucionada la contingencia y recuperados los procesos y servicios críticos de la organización, corresponderá volver a la normalidad de funcionamiento y operación.

Este plan de vuelta a normalidad implica recuperar el sitio y los equipos tecnológicos del centro de operación y control de la Central Paute Mazar.

Para el efecto el CPCI deberá:

1. Realizar un resumen del estado del evento.
2. Evaluar el estado de los activos.
3. Coordinar con las diferentes áreas de la organización, la reparación o adquisición de repuestos necesarios tanto de

la parte física como de la parte tecnológica del centro de control Paute-Mazar.

4. Dar seguimiento y vigilar el cumplimiento del punto 1.
5. Informar al comité de crisis del avance de retorno de vuelta a la normalidad del centro de control Paute-Mazar.
6. Finalizada la reparación o adquisición de los repuestos necesarios, deberá coordinar con los diferentes equipos SPMZ, RCMZ, OPMZ y diferentes áreas de la organización la instalación de los nuevos recursos tecnológicos en el centro de control de Paute-Mazar.
7. Finalizado el punto 4, deberá coordinar con los equipos SPMZ, RCMZ, OPMZ el retorno del control de la operación de Paute-Mazar, desde las instalaciones habituales.
8. Informar al Comité de crisis de la finalización del retorno de vuelta a la normalidad del centro de control de Paute-Mazar.
9. Evaluar los resultados.

4.4 Definir y documentar los procedimientos de recuperación

Tomando en cuenta la naturaleza de la plataforma tecnología de TIC (Paute-Mazar sistema SCADA) con el fin de tener la información y documentación necesaria cuando exista la presencia

de un evento que afecte parcial o totalmente la misma, se define los siguientes documentos de los procesos de recuperación Anexo E:

a) Indisponibilidad total por Incendio.
b) Indisponibilidad total por Inundación.
c) Indisponibilidad total de suministro eléctrico.
d) Indisponibilidad total de CIS10, C30 Mazar y C30 Molino.
e) Indisponibilidad total de PCX 1 y 2.
f) Indisponibilidad total de Red S8000 1 y 2.
g) Indisponibilidad total de Red F8000 1 y 2.

Es importante recalcar que se deberá dar prioridad a todos los elementos que están presentes en los procesos críticos de la organización (Operación Paute-Mazar).

En estos procedimientos se deberá incorporar detalladamente toda la información pertinente con el fin de recuperar todos los activos de información de los procesos críticos de la de la organización.

El Líder de cada equipo es responsable de elaborar y mantener esta documentación tomado en cuenta siempre el peor escenario de la contingencia.

En la Figura 4.4 se pueden observar como quedarían establecidos los procedimientos de recuperación.

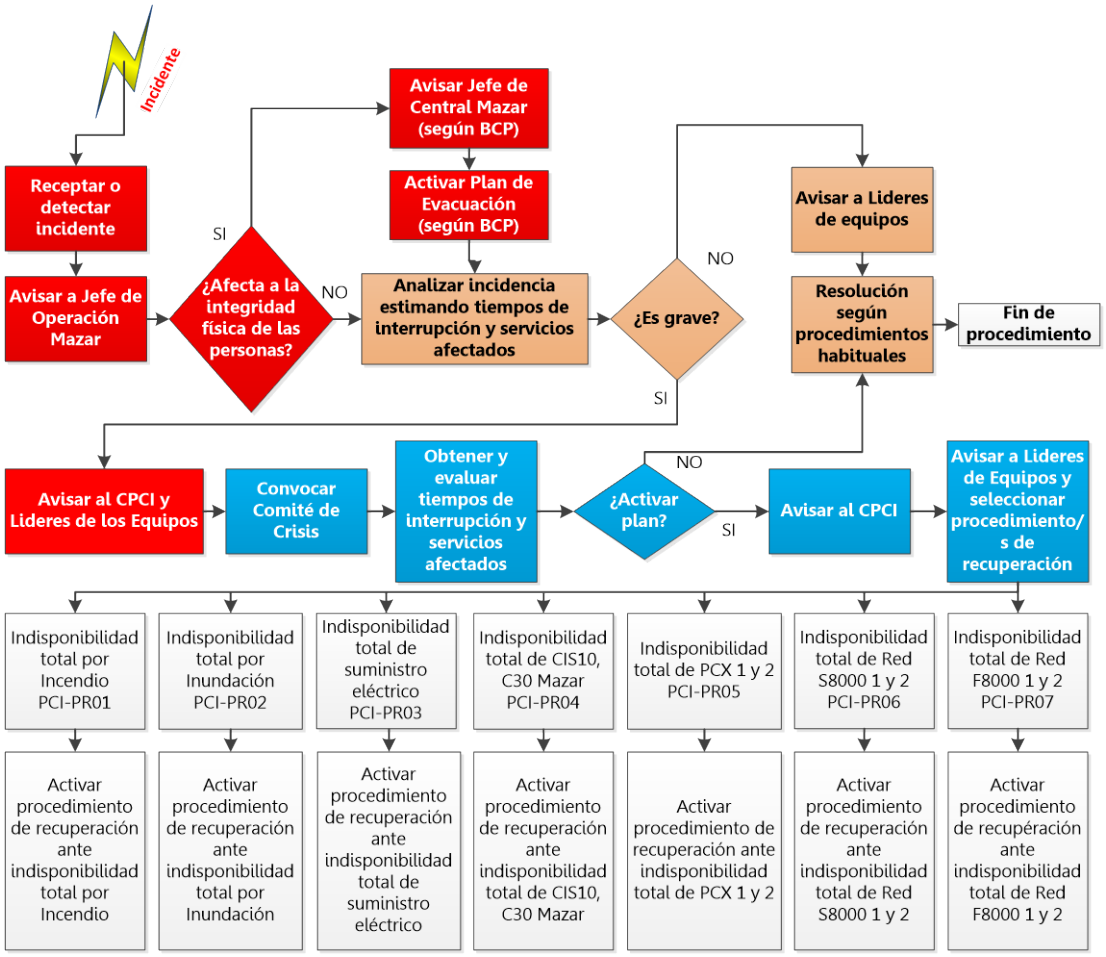


Figura 4.4. Procedimientos de recuperación

Fuente: (INTECO, 2010)

Elaborado por: Alfredo Carpio

4.5 Desarrollar los requerimientos de documentos a utilizar durante y después del desastre

Como parte de los documentos necesarios a utilizarse durante y después del desastre, se definen los siguientes:

Durante:

- ✓ Equipo del Plan de Contingencia Informático

  Se utilizará este formulario (Anexo F) para obtener información de los funcionarios integrantes del plan, que están conformando los diferentes equipos de recuperación, de esta manera se podrá localizarlos con mayor facilidad y sin pérdida de tiempo, en caso de tener una contingencia.

- ✓ Información de contactos externos

  Se utilizará este formulario (Anexo G) para registrar los datos de las entidades externas como la Policía, Bomberos, Proveedores, etc., quiénes podrán ayudar en caso de requerir su colaboración ya sea de manera directa o con la entrega de equipos o repuestos de manera urgente.

- ✓ Procedimientos de recuperación

  Estos procedimientos de recuperación establecidos en el Item 4.4 se utilizarán cuando se haya activado el plan, esto

permitirá a los equipos actuar de manera adecuada para recuperar procesos y servicios críticos.

Después:

- ✓ Resumen del estado de la contingencia

  Se utilizará este formulario (Anexo D) para realizar el seguimiento del estado y evolución de la contingencia, lo que servirá al CPCI para poder comunicar y brindar información del estado y desarrollo de recuperación de la contingencia.

- ✓ Evaluar estado del Activo

  Se utilizará este formulario (Anexo H) para realizar una evaluación de daños ocasionados por la contingencia, de esta manera se podrá definir con mayor precisión qué acciones tomar sobre dicho activo ya sea para su reparación o declararlo como pérdida total ante la aseguradora.

- ✓ Evaluación de Resultados

  Se utilizará este formulario (Anexo I) para realizar una evaluación de las acciones tomadas en la contingencia y poder definir con certeza si funcionaron o no, además

permitirá obtener una retroalimentación de porque funciono o no tal o cual acción y como mejorarlo de ser el caso.

4.6 Proponer pruebas y procedimientos de control, distribución, capacitación y mejora continua del plan

Parte de la mejora continua del plan es la de definir y proponer pruebas las cuales en su concepto forman un conjunto de medidas que ponen en evidencia la aplicabilidad adecuada del plan de contingencia, se propone que este plan sea probado periódicamente en virtud de:

- ✓ La ejecución de pruebas servirá para validar el plan así como para encontrar mejoras que posibiliten que el plan se perfeccione.
- ✓ Los procesos de la organización y la relación siempre presente con la tecnología hacen que con el paso del tiempo pueda quedar obsoleto el plan y no ajustado a los cambios y requerimientos que experimenta la organización.

- ✓ Estas pruebas permiten la posibilidad de evaluar a ciencia cierta cómo responde la organización ante un determinado desastre.
- ✓ Las pruebas deberán tratar de ser concebidas y ajustadas a eventos muy similares que pudiesen ocurrir en la realidad debiendo ser planificadas de tal manera que no afecte las actividades normales de la organización o su riesgo sea mínimo.
- ✓ Deberá programarse un calendario de pruebas en el formulario correspondiente (Anexo J) que será consensuado y comunicado a las áreas pertinentes.

El responsable de las pruebas del plan será el CPCI quién debe velar por el cumplimiento y realización del mismo, así como obtener resultados y conclusiones respecto de:

- ✓ Información a corregir por deficiencias o errores detectados en las pruebas.
- ✓ Información que pudiese requerir de más claridad y exactitud.
- ✓ Información que permita incorporar inconvenientes o riesgos no previstos inicialmente.

- ✓ Información de si los procedimientos establecidos son prácticos y viables.

El CPCI deberá informar de los resultados del plan al representante del comité de crisis y líderes de equipos de recuperación, además de:

- ✓ Definir el calendario de pruebas.
- ✓ Definir el tipo de prueba a utilizar.
- ✓ Definir el alcance y objetivos de las pruebas.
- ✓ Asegurar la actualización del plan, que sea permanente y siempre utilizar la última versión previa a las pruebas.
- ✓ Definir los costos asociados a las pruebas de ser el caso.
- ✓ Mantener reuniones con las áreas, departamentos y equipos de recuperación involucrados en las pruebas, previas y posteriores a la realización de la pruebas del plan.
- ✓ Definir plan de capacitación que garantice a los funcionarios involucrados en el plan obtener las competencias necesarias en su ámbito de acción.

En la Tabla 31 se establece la propuesta de pruebas al plan de contingencia.

Tabla 31. Pruebas del Plan

TIPO DE PRUEBA	DESCRIPCIÓN	FRECUENCIA
CONSISTENCIA	Distribución del plan de contingencia a las áreas funcionales involucradas para revisión y/o actualización.	Anual
VALIDEZ	Reunión con involucrados de las áreas de Operación, Redes y Comunicaciones y Soluciones de Producción para revisar y discutir el plan.	Previo a simulación
SIMULACIÓN	Se prepara un ambiente idéntico al real de una contingencia para identificar si el plan contiene la información necesaria y suficiente.	Previo actividad crítica
ACTIVIDADES CRITICAS	En un entorno controlado que no afecte la operación de la organización, realizar una recuperación de un proceso o actividad crítica.	Semestral
COMPLETO	Prueba integral y completa en tiempo real (si fuese posible) en base a los procedimientos que se establecieron previamente en el plan de contingencia.	Anual

Fuente: Propia

Elaborado: Alfredo Carpio

Las pruebas a su vez permitirán descubrir las necesidades y requerimientos de capacitación de los diferentes funcionarios que intervienen en el plan, permitiendo corregir o mejorar las competencias en el ámbito de acción de cada uno de los funcionarios, pero existe también la necesidad de capacitar y difundir el plan al resto de funcionarios de la organización de tal manera de fomentar una cultura y aceptación del cambio, estando de esta manera preparados en caso de requerir su colaboración.

Estas capacitaciones deben enfocarse a:

- ✓ Todos los componentes del plan de contingencia.
- ✓ La importancia de establecer y mantener un plan de contingencia.
- ✓ Identificación de los equipos de recuperación y sus miembros.
- ✓ Características, alcance, objetivos del plan de contingencia.
- ✓ Cómo y quién puede activar el plan de contingencia.

La difusión y concientización del plan se lo podrá realizar desde diferentes medios como:

- ✓ Sitio web Intranet.

- ✓ Videos.
- ✓ Capsulas informativas.
- ✓ Correo electrónico.
- ✓ Afiches.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. Uno de los principales desafíos de hoy en día de las organizaciones es la de estar preparadas ante las contingencias informáticas que se presenten, pues la tecnología va de la mano con sus procesos, esto no es ajeno a la Unidad de Negocio Hidropaute.

2. El compromiso con las partes interesadas así como los requerimientos regulatorios, son factores que están presentes en el día a día de las organizaciones, por ende deben ser resistentes “resiliencia” ante cualquier contingencia que perturbe la entrega del servicio o producto que esta ofrece al mercado.

3. Incorporar un Plan de Contingencia en la organización tiene su impacto, el cual se ve reflejado tanto en las funciones y responsabilidades que dé él se desprenden hacia los funcionarios involucrados en el mismo.

4. El incremento de medidas que garanticen la disponibilidad de los servicios informáticos en la organización permitirán que se logre generar confianza y credibilidad de los usuarios y las partes interesadas.

5. Siempre hay que recalcar que en un Plan de Contingencia no es un gasto, más bien es una inversión que permitirá mantener la entrega del servicio o producto siempre disponible.

6. De nada sirve tener un documento formal de Plan de Contingencia si a este no se lo mantiene prueba y actualiza de manera continua, tal cual lo indica la norma 27001:2013 y buenas prácticas como ITIL, COBIT y el estándar NIST.

Recomendaciones

1. La organización debe analizar esta propuesta de Plan de Contingencia Informática, poniendo énfasis en determinar su idoneidad y factibilidad de incorporarlo al interior de la misma en un tiempo prudente y razonable, ya que en esta propuesta se establecen una serie de medidas técnicas, organizativas y procedimentales con el fin de estar preparada ante una contingencia.

2. Realizar las pruebas y evaluaciones respectivas del plan de contingencia propuesto en la organización.

3. Desarrollar campañas de sensibilización a los funcionarios de la organización orientadas a concienciar sobre sus deberes y responsabilidades en especial a los funcionarios involucrados en los procesos críticos de la organización.

4. Actualizar la información de los funcionarios y proveedores oportunamente, cargos, funciones, responsabilidades, direcciones,

teléfonos, etc., lo cual deberá ser cotejada y actualizada con la información recabada en el plan de contingencia.

5. Difundir adecuadamente el plan de contingencia a los funcionarios y partes interesadas de la organización.

6. El Talento Humano es un factor importante y en ese ámbito el poder contar con personal altamente comprometido y a disposición amerita la necesidad de incorporar a tiempo completo personal tanto en el área de Soluciones de Producción (uno) como de Comunicación y Redes (uno) que garantice el cumplimiento del plan.

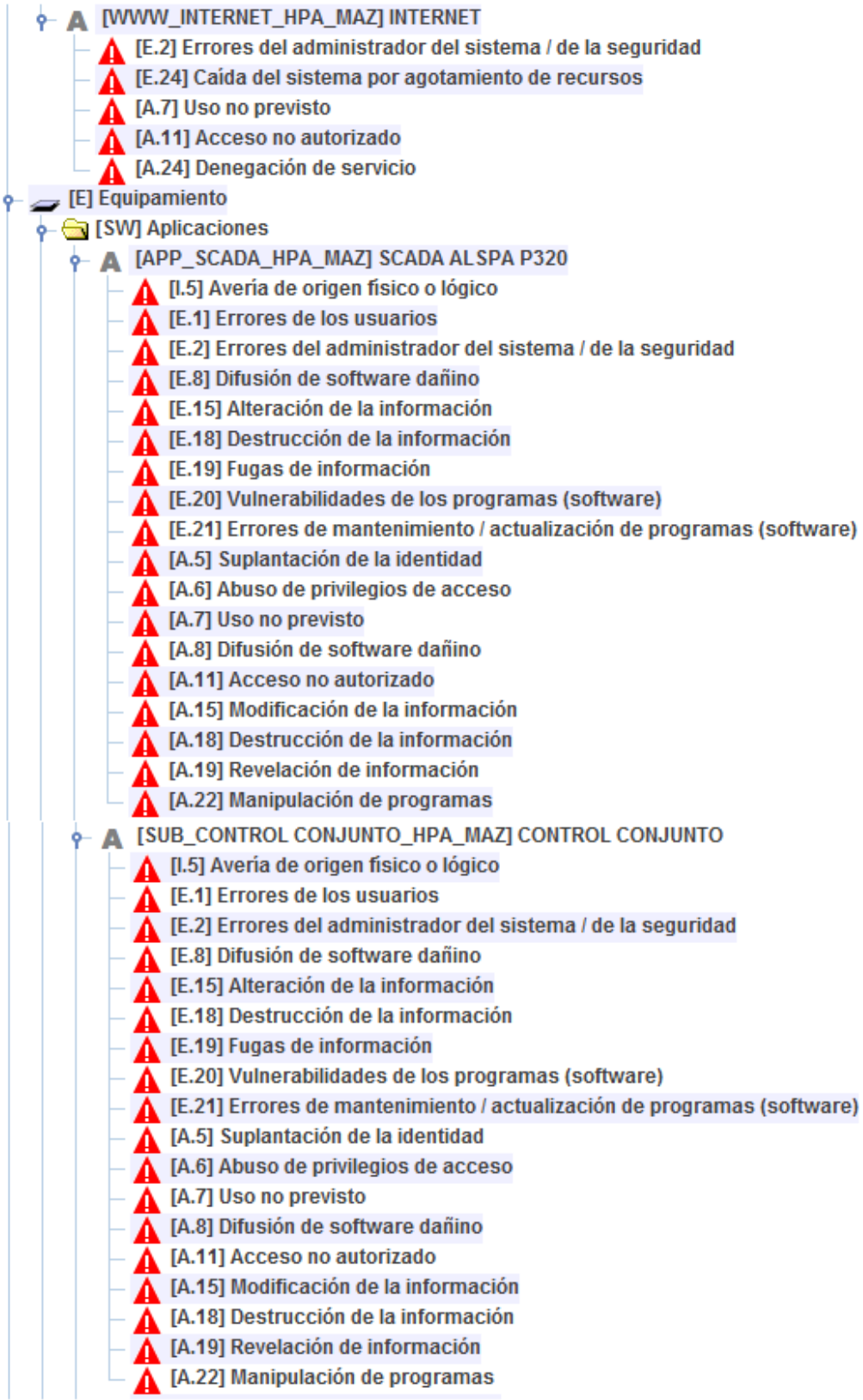
7. Tomar este plan de contingencia como base para ampliar su alcance a las dependencias donde funciona la sede administrativa y la planta de producción Paute-Molino.

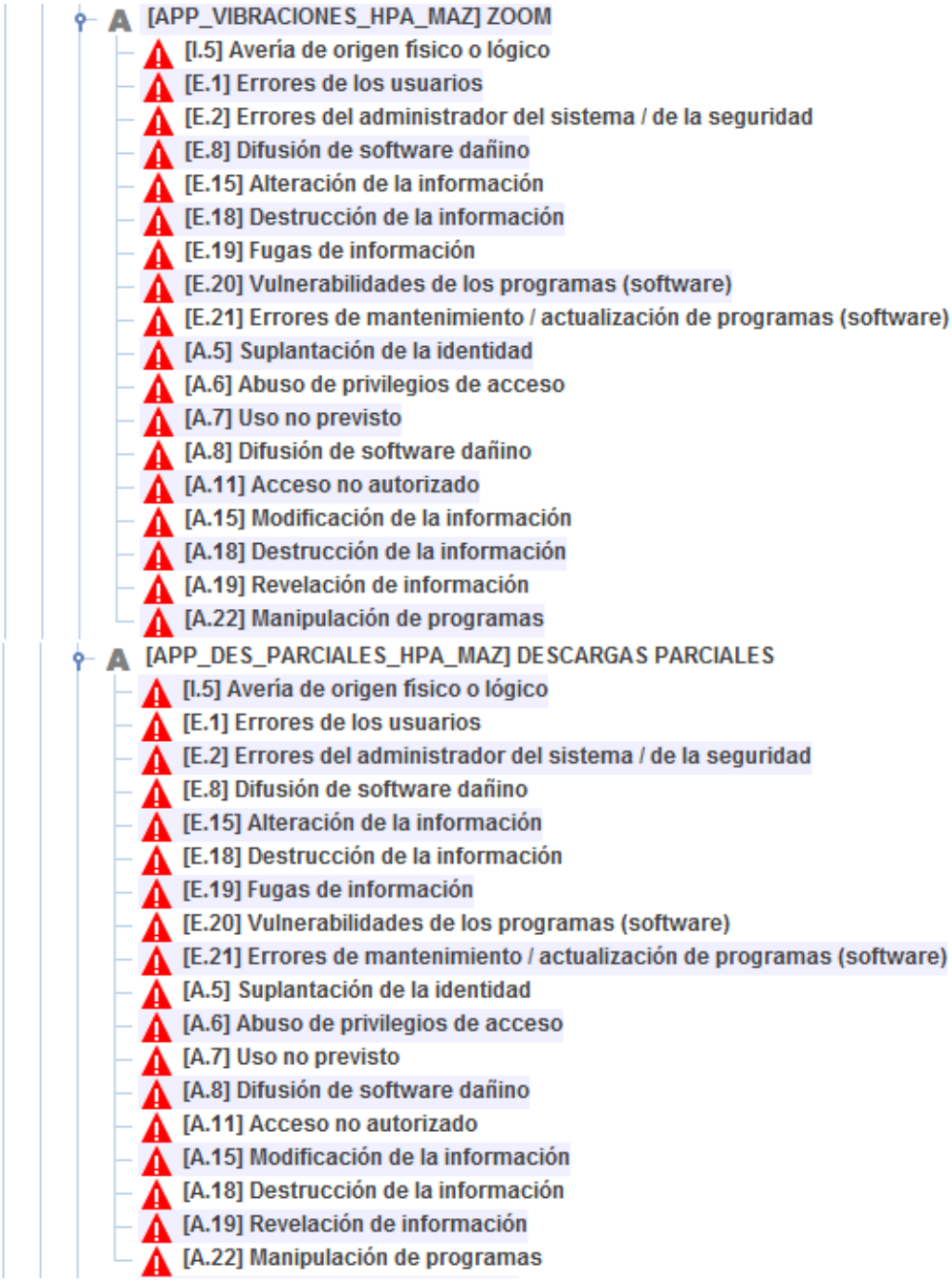
ANEXO A

2014																							
ENE		FEB		MAR		ABR		MAY		JUN		JUL		AGO		SEP		OCT		NOV		DIC	
U01	U02	U01	U02	U01	U02	U01	U02	U01	U02	U01	U02	U01	U02	U01	U02	U01	U02	U01	U02	U01	U02	U01	U02
70.00	70.00	75.00	75.00	70.00	70.00	80.00	80.00	77.50	77.50	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
70.00	70.00	59.64	76.02	70.00	70.00	80.00	80.00	77.50	77.50	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
70.00	70.00	70.00	70.00	70.00	70.00	80.00	80.00	77.50	77.50	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
70.00	70.00	70.00	70.00	70.00	70.00	80.00	80.00	77.50	77.50	85.00	85.00	85.00	85.00	75.16	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
70.00	70.00	70.00	70.00	70.00	70.00	80.00	80.00	77.50	77.50	85.00	85.00	85.00	85.00	0.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
70.00	70.00	70.00	70.00	70.00	70.00	80.00	80.00	77.50	77.50	85.00	85.00	85.00	85.00	0.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
70.00	70.00	70.00	70.00	70.00	70.00	80.00	80.00	77.50	77.50	85.00	85.00	85.00	85.00	0.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
70.00	70.00	70.00	70.00	70.00	70.00	80.00	80.00	77.50	77.50	85.00	85.00	85.00	85.00	0.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
70.00	70.00	70.00	70.00	70.00	70.00	80.00	80.00	77.50	77.50	85.00	85.00	85.00	85.00	0.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
72.20	77.13	70.00	70.00	70.00	70.00	80.00	80.00	77.50	77.50	85.00	85.00	85.00	85.00	0.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
75.00	77.00	70.00	70.00	71.60	71.60	80.00	80.00	82.98	82.98	85.00	85.00	85.00	85.00	0.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
75.00	75.00	70.24	66.69	75.00	75.00	77.50	77.50	83.33	83.33	85.00	85.00	85.00	85.00	0.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
75.00	75.00	70.00	70.00	75.00	75.00	77.50	77.50	85.00	85.00	85.00	85.00	85.00	85.00	0.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
75.00	75.00	70.00	70.00	75.00	75.00	75.00	75.00	85.00	85.00	85.00	85.00	85.00	85.00	0.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
78.44	23.44	70.00	70.00	75.00	75.00	75.00	75.00	85.00	85.00	85.00	85.00	70.54	85.00	0.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
80.00	0.00	70.00	70.00	75.00	75.00	72.50	72.50	85.00	85.00	85.00	85.00	85.00	85.00	0.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
80.00	0.00	70.00	70.00	75.00	75.00	72.50	72.50	85.00	85.00	85.00	85.00	85.00	85.00	0.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
25.00	0.00	70.00	70.00	75.00	75.00	72.50	72.50	85.00	85.00	85.00	85.00	85.00	85.00	27.63	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
26.06	0.00	70.00	70.00	75.00	75.00	72.50	72.50	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
80.00	0.00	70.00	70.00	75.00	75.00	72.50	72.50	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
80.00	0.00	70.00	70.00	75.00	75.00	72.50	72.50	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
80.00	3.78	70.00	70.00	75.00	75.00	75.00	75.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
75.00	75.00	70.00	70.00	75.00	75.00	75.00	75.00	85.00	85.00	78.80	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
75.00	75.00	70.00	70.00	75.00	75.00	75.00	75.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
75.00	78.82	70.00	70.00	80.00	80.00	75.00	75.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
75.00	74.58	70.00	70.00	80.00	80.00	75.00	75.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
75.00	75.00	67.08	70.63	80.00	80.00	75.00	75.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
75.00	75.00	60.76	71.98	80.00	80.00	77.50	77.50	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
75.00	75.00			80.00	80.00	77.50	77.50	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
75.00	75.00			80.00	80.00	77.50	77.50	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00	85.00
75.00	75.00			80.00	80.00			85.00	85.00			85.00	85.00	85.00	85.00			85.00	85.00			85.00	85.00
126.50		139.75		148.81		153.50		164.92		169.79		169.53		132.19		170.00		170.00		170.00		170.00	

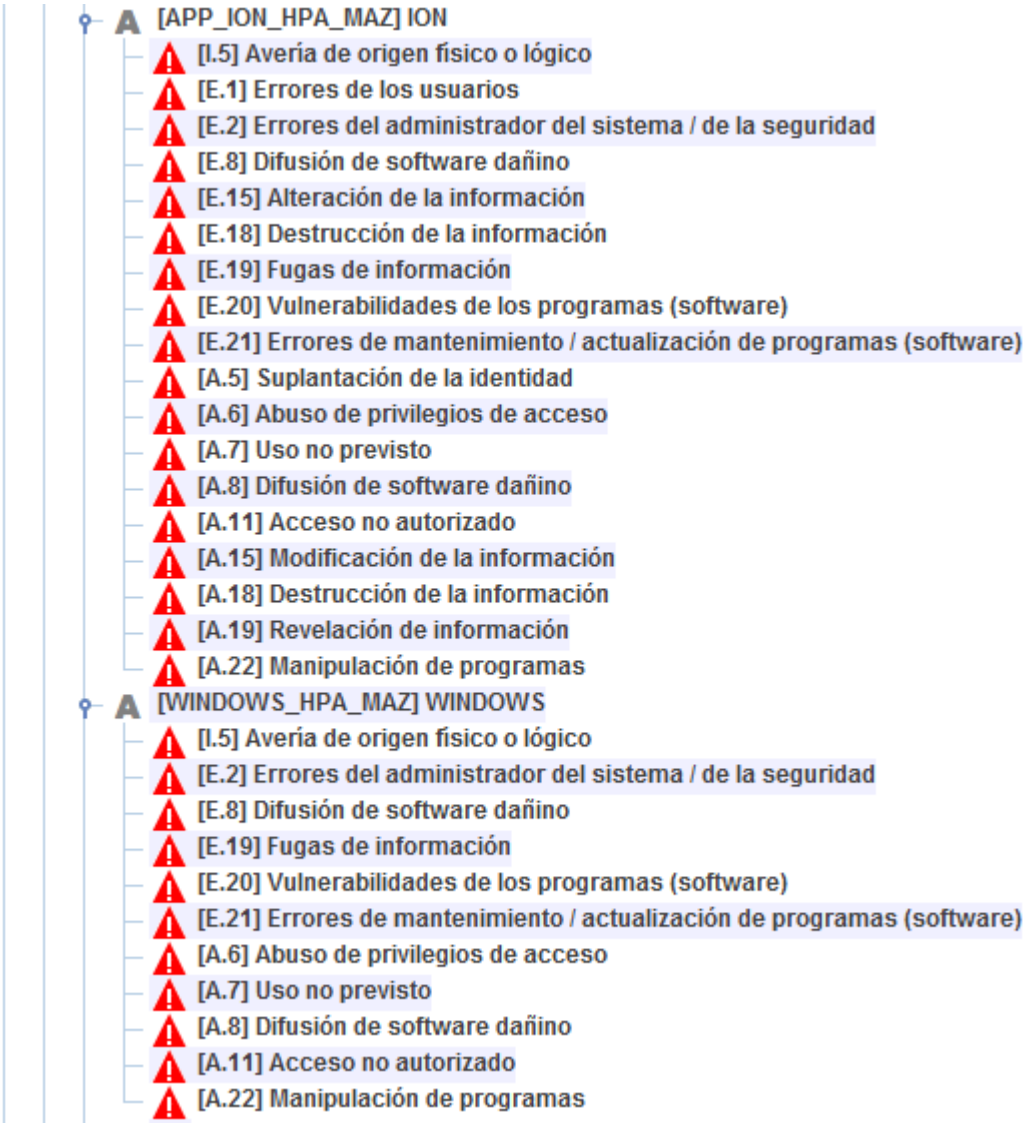
ANEXO B

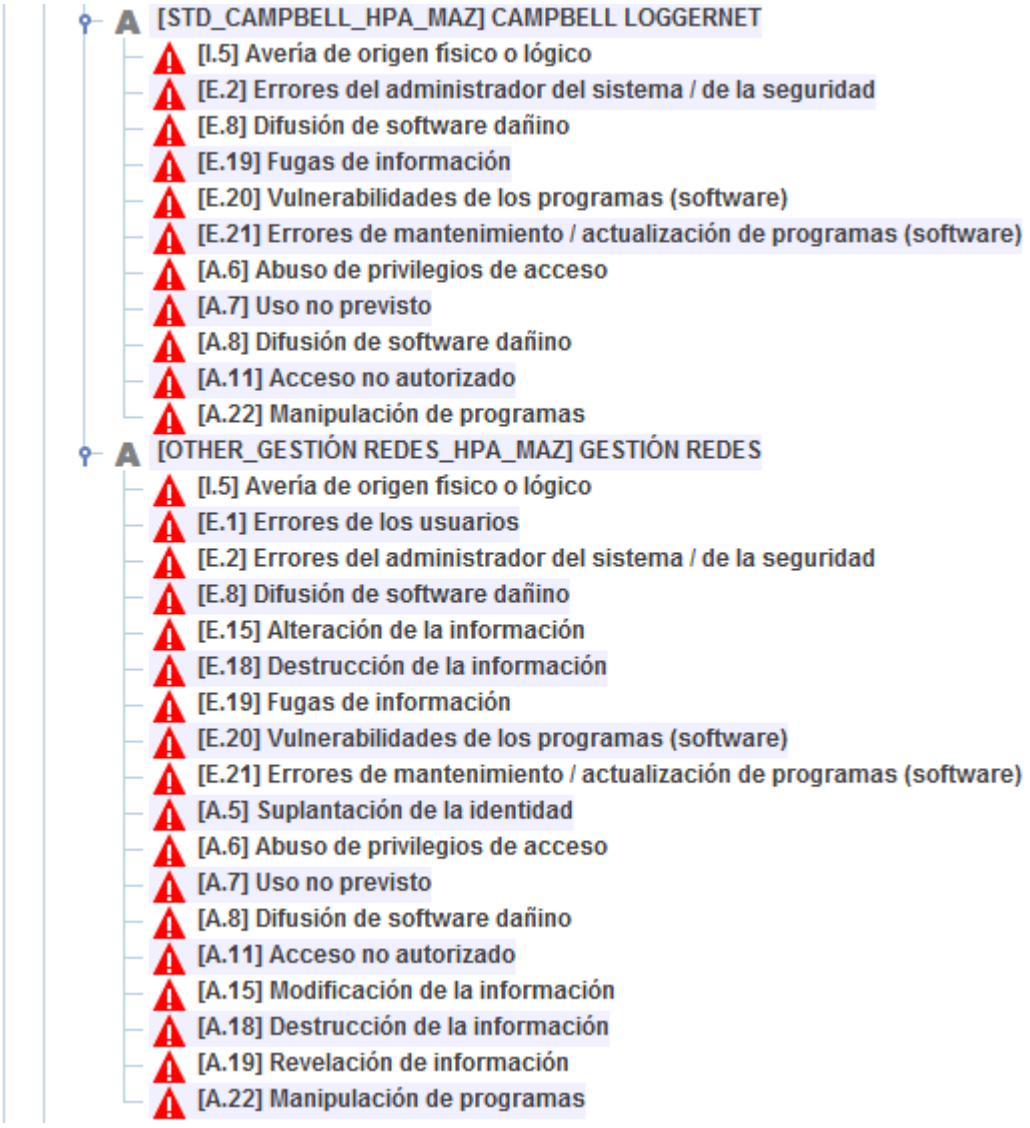

HPA_MAZAR: Identificación de las amenazas - [eval] alfredo
TSV
3
+1
sugiere
amenaza
ACTIVOS
[B] Activos esenciales
[SCADA_HPA_MAZAR] SCADA AL SPA P320 MAZAR
[N.*.4] Terremotos
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3.3] Polvo
[I.5] Avería de origen físico o lógico
[I.5.1] Software
[I.5.2] Hardware
[I.5.3] Equipos de comunicaciones
[I.5.4] Equipamiento auxiliar
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.11] Emanaciones electromagnéticas
[E.2] Errores del administrador del sistema / de la seguridad
[E.4] Errores de configuración
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.23] Manipulación del hardware
[IS] Servicios internos
[VOIP_TELEF_ IP_HPA_MAZ] TELEFONIA IP
[E.1] Errores de los usuarios
[E.2] Errores del administrador del sistema / de la seguridad
[E.24] Caída del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.24] Denegación de servicio
[A.28.1] Enfermedad
[MOBILE_TELEF_ DECT_HPA_MAZ] TELEFONIA MOVIL
[E.1] Errores de los usuarios
[E.2] Errores del administrador del sistema / de la seguridad
[E.24] Caída del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.24] Denegación de servicio
[A.28.1] Enfermedad
[INT_CCTV_ HPA_MAZ] CCTV VIDEOVIGILANCIA
[E.1] Errores de los usuarios
[E.2] Errores del administrador del sistema / de la seguridad
[E.24] Caída del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.24] Denegación de servicio
[A.28.1] Enfermedad

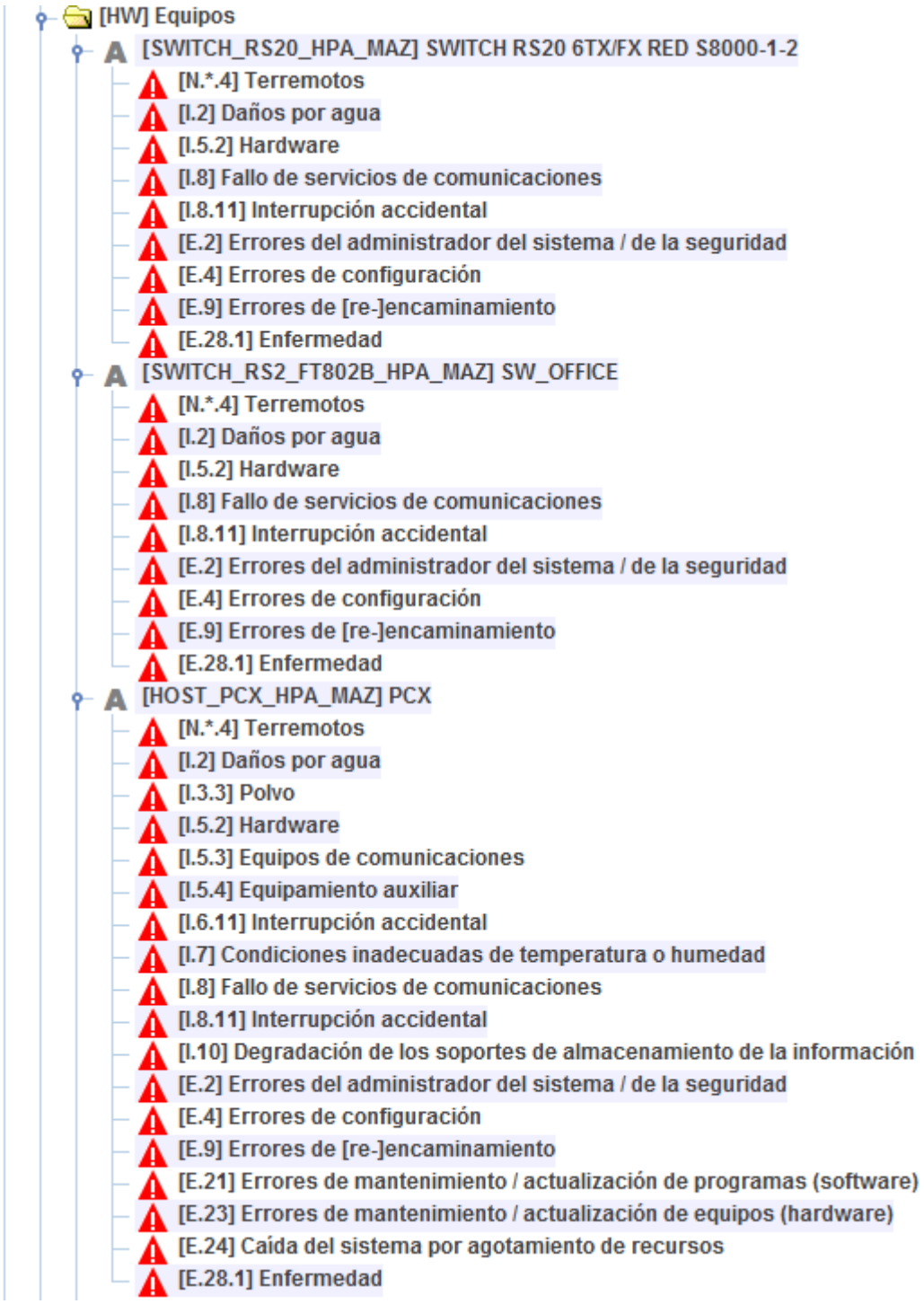

[WWW_INTERNET_HPA_MAZ] INTERNET
[E.2] Errores del administrador del sistema / de la seguridad
[E.24] Caída del sistema por agotamiento de recursos
[A.7] Uso no previsto
[A.11] Acceso no autorizado
[A.24] Denegación de servicio
[E] Equipamiento
[SW] Aplicaciones
[APP_SCADA_HPA_MAZ] SCADA ALSPA P320
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador del sistema / de la seguridad
[E.8] Difusión de software dañino
[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[A.5] Suplantación de la identidad
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.11] Acceso no autorizado
[A.15] Modificación de la información
[A.18] Destrucción de la información
[A.19] Revelación de información
[A.22] Manipulación de programas
[SUB_CONTROL CONJUNTO_HPA_MAZ] CONTROL CONJUNTO
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador del sistema / de la seguridad
[E.8] Difusión de software dañino
[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[A.5] Suplantación de la identidad
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.11] Acceso no autorizado
[A.15] Modificación de la información
[A.18] Destrucción de la información
[A.19] Revelación de información
[A.22] Manipulación de programas

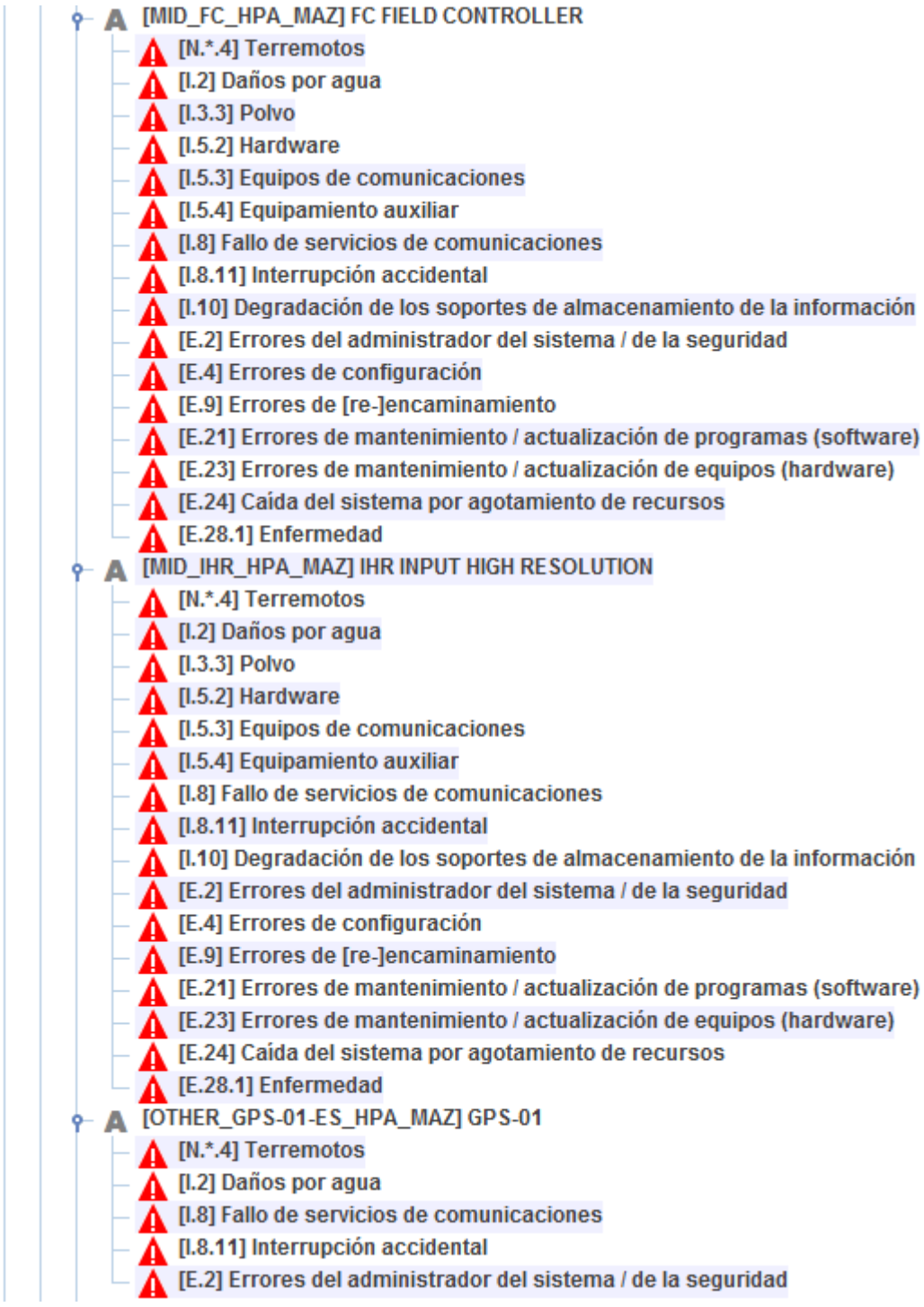

[APP_VIBRACIONES_HPA_MAZ] ZOOM
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador del sistema / de la seguridad
[E.8] Difusión de software dañino
[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[A.5] Suplantación de la identidad
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.11] Acceso no autorizado
[A.15] Modificación de la información
[A.18] Destrucción de la información
[A.19] Revelación de información
[A.22] Manipulación de programas
[APP_DES_PARCIALES_HPA_MAZ] DESCARGAS PARCIALES
[I.5] Avería de origen físico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador del sistema / de la seguridad
[E.8] Difusión de software dañino
[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[A.5] Suplantación de la identidad
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.11] Acceso no autorizado
[A.15] Modificación de la información
[A.18] Destrucción de la información
[A.19] Revelación de información
[A.22] Manipulación de programas

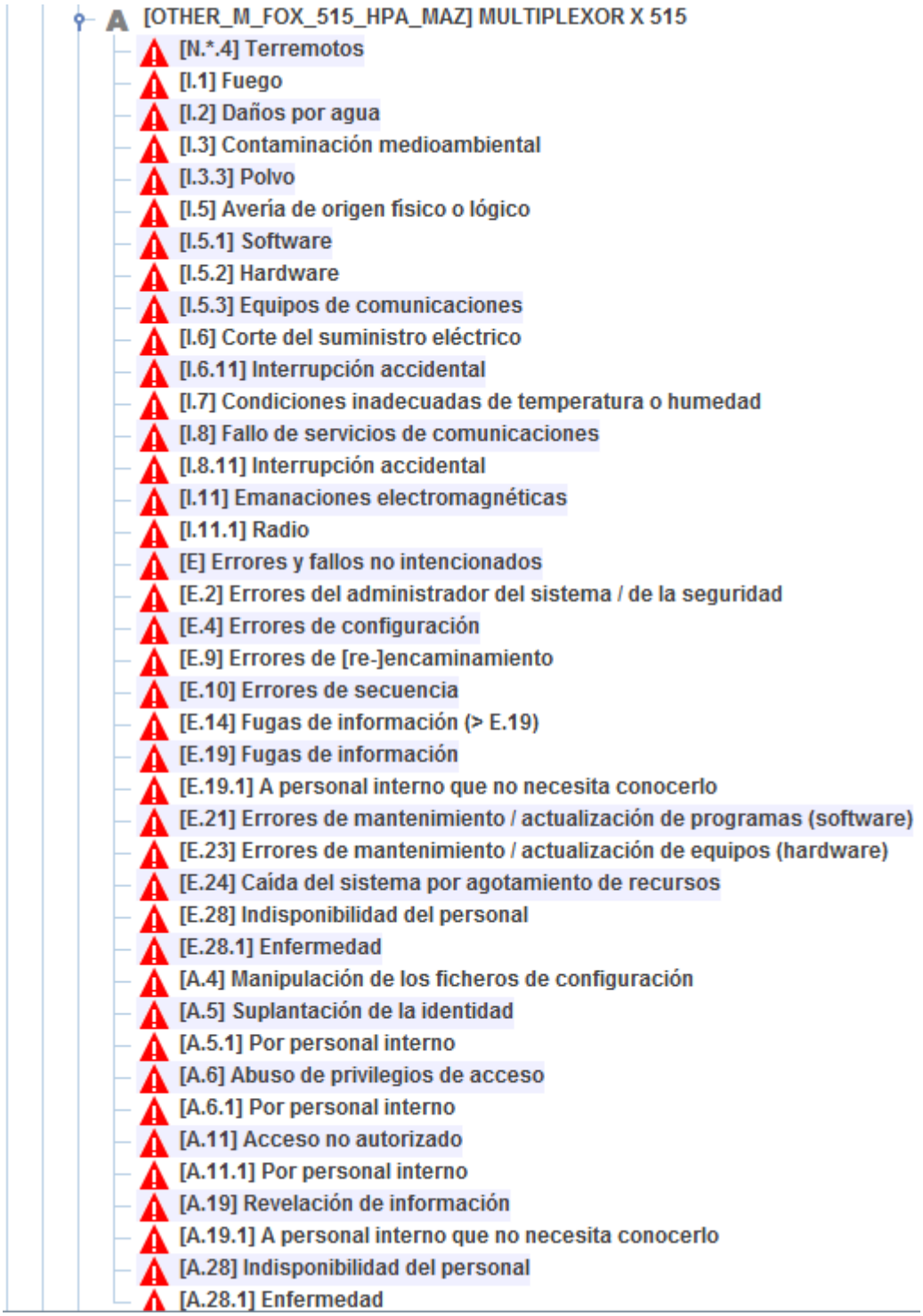
- [PRP_AROCHE_HPA_MAZ] AROCHE
  - [I.5] Avería de origen físico o lógico
  - [I.5.1] Software
  - [E.2] Errores del administrador del sistema / de la seguridad
  - [E.8] Difusión de software dañino
  - [E.15] Alteración de la información
  - [E.18] Destrucción de la información
  - [E.19] Fugas de información
  - [E.20] Vulnerabilidades de los programas (software)
  - [E.21] Errores de mantenimiento / actualización de programas (software)
  - [A.5] Suplantación de la identidad
  - [A.6] Abuso de privilegios de acceso
  - [A.11] Acceso no autorizado
  - [A.15] Modificación de la información
  - [A.22] Manipulación de programas
- [AV_HPA_MAZ] McAfee
  - [I.5] Avería de origen físico o lógico
  - [E.1] Errores de los usuarios
  - [E.2] Errores del administrador del sistema / de la seguridad
  - [E.8] Difusión de software dañino
  - [E.15] Alteración de la información
  - [E.18] Destrucción de la información
  - [E.19] Fugas de información
  - [E.20] Vulnerabilidades de los programas (software)
  - [E.21] Errores de mantenimiento / actualización de programas (software)
  - [A.5] Suplantación de la identidad
  - [A.6] Abuso de privilegios de acceso
  - [A.7] Uso no previsto
  - [A.8] Difusión de software dañino
  - [A.11] Acceso no autorizado
  - [A.15] Modificación de la información
  - [A.18] Destrucción de la información
  - [A.19] Revelación de información
  - [A.22] Manipulación de programas
- [PRP_SCAD_HPA_MAZ] SCAD
  - [I.5] Avería de origen físico o lógico
  - [I.5.1] Software
  - [E.2] Errores del administrador del sistema / de la seguridad
  - [E.8] Difusión de software dañino
  - [E.15] Alteración de la información
  - [E.18] Destrucción de la información
  - [E.19] Fugas de información
  - [E.20] Vulnerabilidades de los programas (software)
  - [E.21] Errores de mantenimiento / actualización de programas (software)
  - [A.5] Suplantación de la identidad
  - [A.6] Abuso de privilegios de acceso
  - [A.11] Acceso no autorizado
  - [A.15] Modificación de la información
  - [A.22] Manipulación de programas


[APP_ION_HPA_MAZ] ION
[I.5] Avería de origen fisico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador del sistema / de la seguridad
[E.8] Difusión de software dañino
[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[A.5] Suplantación de la identidad
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.11] Acceso no autorizado
[A.15] Modificación de la información
[A.18] Destrucción de la información
[A.19] Revelación de información
[A.22] Manipulación de programas
[WINDOWS_HPA_MAZ] WINDOWS
[I.5] Avería de origen fisico o lógico
[E.2] Errores del administrador del sistema / de la seguridad
[E.8] Difusión de software dañino
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.11] Acceso no autorizado
[A.22] Manipulación de programas


[STD_CAMPBELL_HPA_MAZ] CAMPBELL LOGGERNET
[I.5] Avería de origen fisico o lógico
[E.2] Errores del administrador del sistema / de la seguridad
[E.8] Difusión de software dañino
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.11] Acceso no autorizado
[A.22] Manipulación de programas
[OTHER_GESTIÓN REDES_HPA_MAZ] GESTIÓN REDES
[I.5] Avería de origen fisico o lógico
[E.1] Errores de los usuarios
[E.2] Errores del administrador del sistema / de la seguridad
[E.8] Difusión de software dañino
[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.19] Fugas de información
[E.20] Vulnerabilidades de los programas (software)
[E.21] Errores de mantenimiento / actualización de programas (software)
[A.5] Suplantación de la identidad
[A.6] Abuso de privilegios de acceso
[A.7] Uso no previsto
[A.8] Difusión de software dañino
[A.11] Acceso no autorizado
[A.15] Modificación de la información
[A.18] Destrucción de la información
[A.19] Revelación de información
[A.22] Manipulación de programas


[HW] Equipos
[SWITCH_RS20_HPA_MAZ] SWITCH RS20 6TX/FX RED S8000-1-2
[N.*.4] Terremotos
[I.2] Daños por agua
[I.5.2] Hardware
[I.8] Fallo de servicios de comunicaciones
[I.8.11] Interrupción accidental
[E.2] Errores del administrador del sistema / de la seguridad
[E.4] Errores de configuración
[E.9] Errores de [re-]encaminamiento
[E.28.1] Enfermedad
[SWITCH_RS2_FT802B_HPA_MAZ] SW_OFFICE
[N.*.4] Terremotos
[I.2] Daños por agua
[I.5.2] Hardware
[I.8] Fallo de servicios de comunicaciones
[I.8.11] Interrupción accidental
[E.2] Errores del administrador del sistema / de la seguridad
[E.4] Errores de configuración
[E.9] Errores de [re-]encaminamiento
[E.28.1] Enfermedad
[HOST_PCX_HPA_MAZ] PCX
[N.*.4] Terremotos
[I.2] Daños por agua
[I.3.3] Polvo
[I.5.2] Hardware
[I.5.3] Equipos de comunicaciones
[I.5.4] Equipamiento auxiliar
[I.6.11] Interrupción accidental
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[I.8.11] Interrupción accidental
[I.10] Degradación de los soportes de almacenamiento de la información
[E.2] Errores del administrador del sistema / de la seguridad
[E.4] Errores de configuración
[E.9] Errores de [re-]encaminamiento
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.28.1] Enfermedad

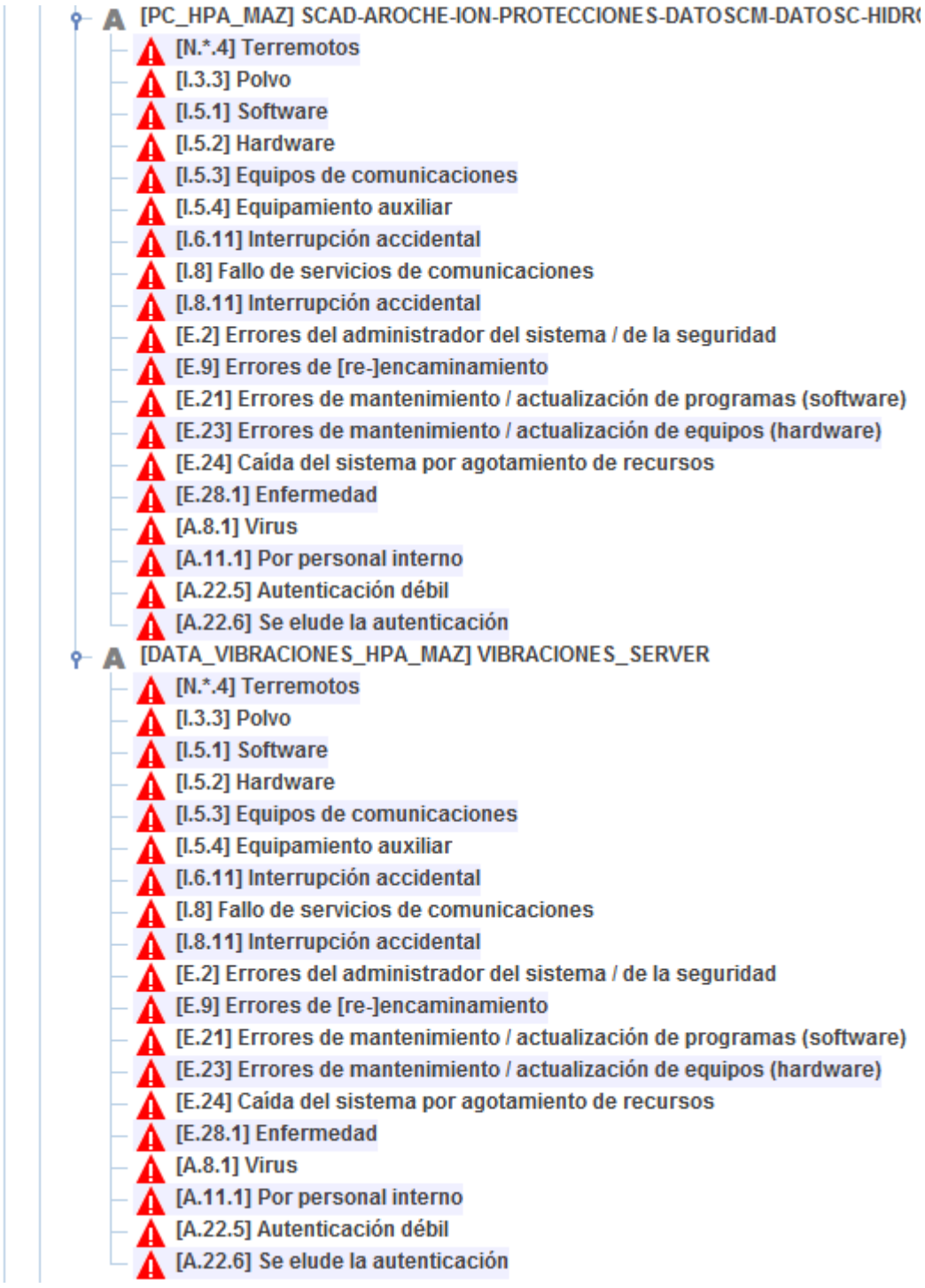

[MID_FC_HPA_MAZ] FC FIELD CONTROLLER
[N.*.4] Terremotos
[I.2] Daños por agua
[I.3.3] Polvo
[I.5.2] Hardware
[I.5.3] Equipos de comunicaciones
[I.5.4] Equipamiento auxiliar
[I.8] Fallo de servicios de comunicaciones
[I.8.11] Interrupción accidental
[I.10] Degradación de los soportes de almacenamiento de la información
[E.2] Errores del administrador del sistema / de la seguridad
[E.4] Errores de configuración
[E.9] Errores de [re-]encaminamiento
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.28.1] Enfermedad
[MID_IHR_HPA_MAZ] IHR INPUT HIGH RESOLUTION
[N.*.4] Terremotos
[I.2] Daños por agua
[I.3.3] Polvo
[I.5.2] Hardware
[I.5.3] Equipos de comunicaciones
[I.5.4] Equipamiento auxiliar
[I.8] Fallo de servicios de comunicaciones
[I.8.11] Interrupción accidental
[I.10] Degradación de los soportes de almacenamiento de la información
[E.2] Errores del administrador del sistema / de la seguridad
[E.4] Errores de configuración
[E.9] Errores de [re-]encaminamiento
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.28.1] Enfermedad
[OTHER_GPS-01-ES_HPA_MAZ] GPS-01
[N.*.4] Terremotos
[I.2] Daños por agua
[I.8] Fallo de servicios de comunicaciones
[I.8.11] Interrupción accidental
[E.2] Errores del administrador del sistema / de la seguridad


[OTHER_M_FOX_515_HPA_MAZ] MULTIPLEXOR X 515
[N.*.4] Terremotos
[I.1] Fuego
[I.2] Daños por agua
[I.3] Contaminación medioambiental
[I.3.3] Polvo
[I.5] Avería de origen físico o lógico
[I.5.1] Software
[I.5.2] Hardware
[I.5.3] Equipos de comunicaciones
[I.6] Corte del suministro eléctrico
[I.6.11] Interrupción accidental
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[I.8.11] Interrupción accidental
[I.11] Emanaciones electromagnéticas
[I.11.1] Radio
[E] Errores y fallos no intencionados
[E.2] Errores del administrador del sistema / de la seguridad
[E.4] Errores de configuración
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.14] Fugas de información (> E.19)
[E.19] Fugas de información
[E.19.1] A personal interno que no necesita conocerlo
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.28] Indisponibilidad del personal
[E.28.1] Enfermedad
[A.4] Manipulación de los ficheros de configuración
[A.5] Suplantación de la identidad
[A.5.1] Por personal interno
[A.6] Abuso de privilegios de acceso
[A.6.1] Por personal interno
[A.11] Acceso no autorizado
[A.11.1] Por personal interno
[A.19] Revelación de información
[A.19.1] A personal interno que no necesita conocerlo
[A.28] Indisponibilidad del personal
[A.28.1] Enfermedad

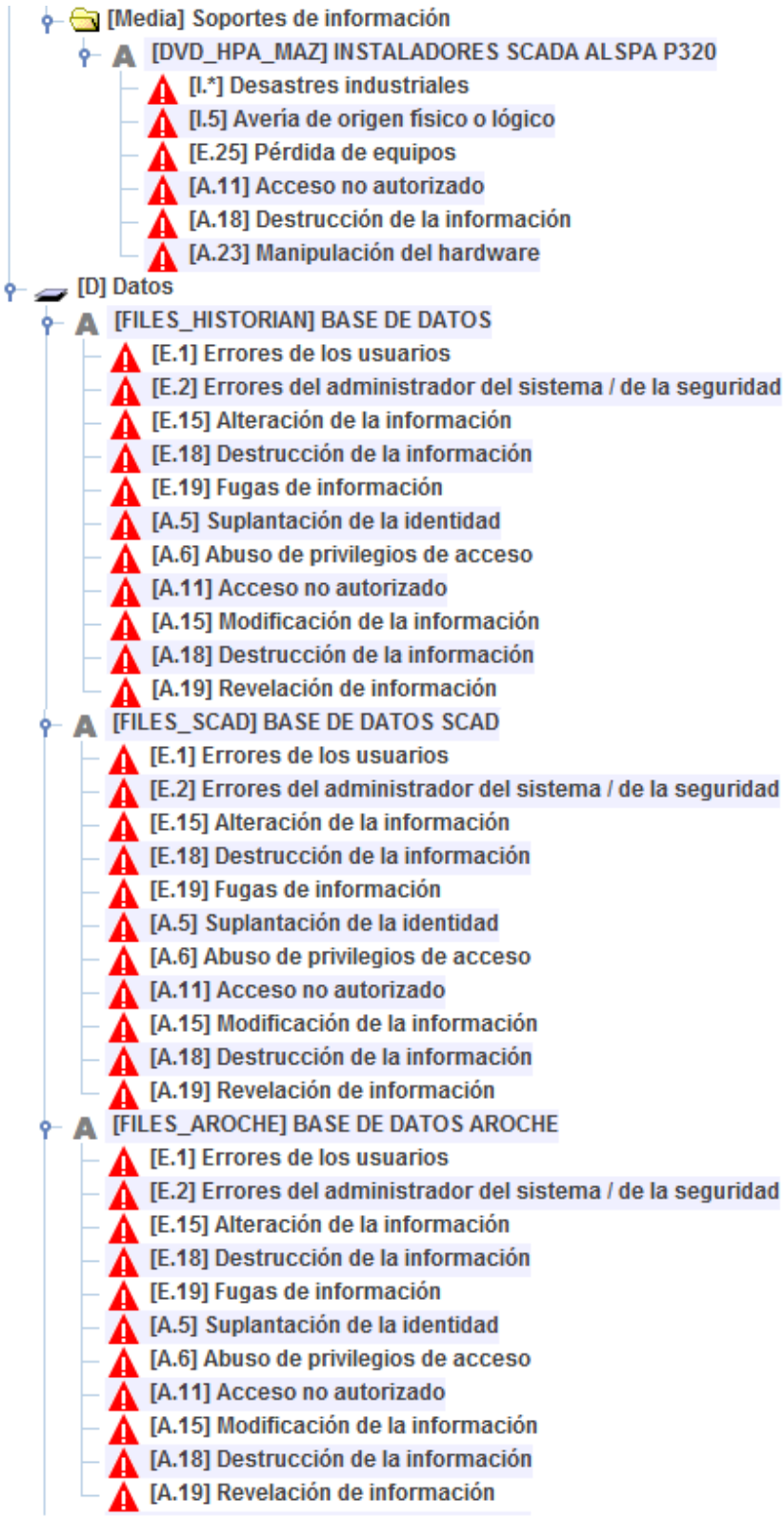

[OTHER_M_UMUX_1500_HPA_MAZ] MULTIPLEXOR UMUX 1500
[N.*.4] Terremotos
[I.1] Fuego
[I.2] Daños por agua
[I.3] Contaminación medioambiental
[I.3.3] Polvo
[I.5] Avería de origen físico o lógico
[I.5.1] Software
[I.5.2] Hardware
[I.5.3] Equipos de comunicaciones
[I.6] Corte del suministro eléctrico
[I.6.11] Interrupción accidental
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[I.8.11] Interrupción accidental
[I.11] Emanaciones electromagnéticas
[I.11.1] Radio
[E] Errores y fallos no intencionados
[E.2] Errores del administrador del sistema / de la seguridad
[E.4] Errores de configuración
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.14] Fugas de información (> E.19)
[E.19] Fugas de información
[E.19.1] A personal interno que no necesita conocerlo
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.28] Indisponibilidad del personal
[E.28.1] Enfermedad
[A.4] Manipulación de los ficheros de configuración
[A.5] Suplantación de la identidad
[A.5.1] Por personal interno
[A.6] Abuso de privilegios de acceso
[A.6.1] Por personal interno
[A.11] Acceso no autorizado
[A.11.1] Por personal interno
[A.19] Revelación de información
[A.19.1] A personal interno que no necesita conocerlo
[A.28] Indisponibilidad del personal
[A.28.1] Enfermedad

- [MID_C30_1-3-4_HPA_MAZ] CONSOLA CIS/CVS 1-3-4 MAZAR-MOLINO
  - [N.*.4] Terremotos
  - [I.3.3] Polvo
  - [I.5.1] Software
  - [I.5.2] Hardware
  - [I.5.3] Equipos de comunicaciones
  - [I.5.4] Equipamiento auxiliar
  - [I.6.11] Interrupción accidental
  - [I.8] Fallo de servicios de comunicaciones
  - [I.8.11] Interrupción accidental
  - [E.2] Errores del administrador del sistema / de la seguridad
  - [E.9] Errores de [re-]encaminamiento
  - [E.21] Errores de mantenimiento / actualización de programas (software)
  - [E.23] Errores de mantenimiento / actualización de equipos (hardware)
  - [E.24] Caída del sistema por agotamiento de recursos
  - [E.28.1] Enfermedad
  - [A.8.1] Virus
  - [A.11.1] Por personal interno
  - [A.22.5] Autenticación débil
  - [A.22.6] Se elude la autenticación
- [MID_CCC_HPA_MAZ] CONSOLA CCC MAZAR-MOLINO
  - [N.*.4] Terremotos
  - [I.3.3] Polvo
  - [I.5.1] Software
  - [I.5.2] Hardware
  - [I.5.3] Equipos de comunicaciones
  - [I.5.4] Equipamiento auxiliar
  - [I.6.11] Interrupción accidental
  - [I.8] Fallo de servicios de comunicaciones
  - [I.8.11] Interrupción accidental
  - [E.2] Errores del administrador del sistema / de la seguridad
  - [E.9] Errores de [re-]encaminamiento
  - [E.21] Errores de mantenimiento / actualización de programas (software)
  - [E.23] Errores de mantenimiento / actualización de equipos (hardware)
  - [E.24] Caída del sistema por agotamiento de recursos
  - [E.28.1] Enfermedad
  - [A.8.1] Virus
  - [A.11.1] Por personal interno
  - [A.22.5] Autenticación débil
  - [A.22.6] Se elude la autenticación

- [MID_CONTROCAD_HPA_MAZ] CONTROCAD SERVER MAZAR-MOLINO
  - [N.*.4] Terremotos
  - [I.3.3] Polvo
  - [I.5.1] Software
  - [I.5.2] Hardware
  - [I.5.3] Equipos de comunicaciones
  - [I.5.4] Equipamiento auxiliar
  - [I.6.11] Interrupción accidental
  - [I.8] Fallo de servicios de comunicaciones
  - [I.8.11] Interrupción accidental
  - [E.2] Errores del administrador del sistema / de la seguridad
  - [E.9] Errores de [re-]encaminamiento
  - [E.21] Errores de mantenimiento / actualización de programas (software)
  - [E.23] Errores de mantenimiento / actualización de equipos (hardware)
  - [E.24] Caída del sistema por agotamiento de recursos
  - [E.28.1] Enfermedad
  - [A.8.1] Virus
  - [A.11.1] Por personal interno
  - [A.22.5] Autenticación débil
  - [A.22.6] Se elude la autenticación
- [MID_C10_HPA_MAZ] CONSOLA C10
  - [N.*.4] Terremotos
  - [I.3.3] Polvo
  - [I.5.1] Software
  - [I.5.2] Hardware
  - [I.5.3] Equipos de comunicaciones
  - [I.5.4] Equipamiento auxiliar
  - [I.6.11] Interrupción accidental
  - [I.8] Fallo de servicios de comunicaciones
  - [I.8.11] Interrupción accidental
  - [E.2] Errores del administrador del sistema / de la seguridad
  - [E.9] Errores de [re-]encaminamiento
  - [E.21] Errores de mantenimiento / actualización de programas (software)
  - [E.23] Errores de mantenimiento / actualización de equipos (hardware)
  - [E.24] Caída del sistema por agotamiento de recursos
  - [E.28.1] Enfermedad
  - [A.8.1] Virus
  - [A.11.1] Por personal interno
  - [A.22.5] Autenticación débil
  - [A.22.6] Se elude la autenticación


[PC_HPA_MAZ] SCAD-AROCHE-ION-PROTECCIONES-DATOSCM-DATOSC-HIDR(
[N.*.4] Terremotos
[I.3.3] Polvo
[I.5.1] Software
[I.5.2] Hardware
[I.5.3] Equipos de comunicaciones
[I.5.4] Equipamiento auxiliar
[I.6.11] Interrupción accidental
[I.8] Fallo de servicios de comunicaciones
[I.8.11] Interrupción accidental
[E.2] Errores del administrador del sistema / de la seguridad
[E.9] Errores de [re-]encaminamiento
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.28.1] Enfermedad
[A.8.1] Virus
[A.11.1] Por personal interno
[A.22.5] Autenticación débil
[A.22.6] Se elude la autenticación
[DATA_VIBRACIONES_HPA_MAZ] VIBRACIONES_SERVER
[N.*.4] Terremotos
[I.3.3] Polvo
[I.5.1] Software
[I.5.2] Hardware
[I.5.3] Equipos de comunicaciones
[I.5.4] Equipamiento auxiliar
[I.6.11] Interrupción accidental
[I.8] Fallo de servicios de comunicaciones
[I.8.11] Interrupción accidental
[E.2] Errores del administrador del sistema / de la seguridad
[E.9] Errores de [re-]encaminamiento
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[E.28.1] Enfermedad
[A.8.1] Virus
[A.11.1] Por personal interno
[A.22.5] Autenticación débil
[A.22.6] Se elude la autenticación


[COM] Comunicaciones
[COM_RED S8000] RED S8000-1/2
[N.*.4] Terremotos
[I.8] Fallo de servicios de comunicaciones
[I.8.11] Interrupción accidental
[E.2] Errores del administrador del sistema / de la seguridad
[E.9] Errores de [re-]encaminamiento
[E.28.1] Enfermedad
[COM_RED F8000-1/2] RED F8000-1/2
[N.*.4] Terremotos
[I.8] Fallo de servicios de comunicaciones
[I.8.11] Interrupción accidental
[E.2] Errores del administrador del sistema / de la seguridad
[E.9] Errores de [re-]encaminamiento
[E.28.1] Enfermedad
[COM_RED OFFICE] RED OFFICE
[N.*.4] Terremotos
[I.8] Fallo de servicios de comunicaciones
[I.8.11] Interrupción accidental
[E.2] Errores del administrador del sistema / de la seguridad
[E.9] Errores de [re-]encaminamiento
[E.28.1] Enfermedad
[COM_LAN] RED LAN
[I.8] Fallo de servicios de comunicaciones
[E.2] Errores del administrador del sistema / de la seguridad
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración de la información
[E.19] Fugas de información
[E.24] Caída del sistema por agotamiento de recursos
[A.7] Uso no previsto
[A.9] [Re-]encaminamiento de mensajes
[A.11] Acceso no autorizado
[A.12] Análisis de tráfico
[A.14] Interceptación de información (escucha)
[A.24] Denegación de servicio
[PABX_TELEF_HPA_MAZ] CENTRAL TELEFONICA MAZAR
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación medioambiental
[I.3.3] Polvo
[I.5] Avería de origen físico o lógico
[I.6] Corte del suministro eléctrico
[I.7] Condiciones inadecuadas de temperatura o humedad
[I.8] Fallo de servicios de comunicaciones
[E.2] Errores del administrador del sistema / de la seguridad
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración de la información
[E.19] Fugas de información
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por agotamiento de recursos
[A.23] Manipulación del hardware
[A.24] Denegación de servicio


[Media] Soportes de información
[DVD_HPA_MAZ] INSTALADORES SCADA ALSPA P320
[I.*] Desastres industriales
[I.5] Avería de origen físico o lógico
[E.25] Pérdida de equipos
[A.11] Acceso no autorizado
[A.18] Destrucción de la información
[A.23] Manipulación del hardware
[D] Datos
[FILES_HISTORIAN] BASE DE DATOS
[E.1] Errores de los usuarios
[E.2] Errores del administrador del sistema / de la seguridad
[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.19] Fugas de información
[A.5] Suplantación de la identidad
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación de la información
[A.18] Destrucción de la información
[A.19] Revelación de información
[FILES_SCAD] BASE DE DATOS SCAD
[E.1] Errores de los usuarios
[E.2] Errores del administrador del sistema / de la seguridad
[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.19] Fugas de información
[A.5] Suplantación de la identidad
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación de la información
[A.18] Destrucción de la información
[A.19] Revelación de información
[FILES_AROCHE] BASE DE DATOS AROCHE
[E.1] Errores de los usuarios
[E.2] Errores del administrador del sistema / de la seguridad
[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.19] Fugas de información
[A.5] Suplantación de la identidad
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación de la información
[A.18] Destrucción de la información
[A.19] Revelación de información

- [FILES_VIBRACIONES_HPA_MAZ] ZOOM
  - [E.1] Errores de los usuarios
  - [E.2] Errores del administrador del sistema / de la seguridad
  - [E.15] Alteración de la información
  - [E.18] Destrucción de la información
  - [E.19] Fugas de información
  - [A.5] Suplantación de la identidad
  - [A.6] Abuso de privilegios de acceso
  - [A.11] Acceso no autorizado
  - [A.15] Modificación de la información
  - [A.18] Destrucción de la información
  - [A.19] Revelación de información
- [FILES_ARGIS] BASE DE DATOS PROTECCIONES ARGIS
  - [E.1] Errores de los usuarios
  - [E.2] Errores del administrador del sistema / de la seguridad
  - [E.15] Alteración de la información
  - [E.18] Destrucción de la información
  - [E.19] Fugas de información
  - [A.5] Suplantación de la identidad
  - [A.6] Abuso de privilegios de acceso
  - [A.11] Acceso no autorizado
  - [A.15] Modificación de la información
  - [A.18] Destrucción de la información
  - [A.19] Revelación de información
- [FILES_DESCARGASPARCIALES_HPA_MAZ] DESCARGASPARCIALES
  - [E.1] Errores de los usuarios
  - [E.2] Errores del administrador del sistema / de la seguridad
  - [E.15] Alteración de la información
  - [E.18] Destrucción de la información
  - [E.19] Fugas de información
  - [A.5] Suplantación de la identidad
  - [A.6] Abuso de privilegios de acceso
  - [A.11] Acceso no autorizado
  - [A.15] Modificación de la información
  - [A.18] Destrucción de la información
  - [A.19] Revelación de información
- [FILES_LOGGERNET] BASE DE DATOS LOGGERNET
  - [E.1] Errores de los usuarios
  - [E.2] Errores del administrador del sistema / de la seguridad
  - [E.15] Alteración de la información
  - [E.18] Destrucción de la información
  - [E.19] Fugas de información
  - [A.5] Suplantación de la identidad
  - [A.6] Abuso de privilegios de acceso
  - [A.11] Acceso no autorizado
  - [A.15] Modificación de la información
  - [A.18] Destrucción de la información
  - [A.19] Revelación de información
- [FILES_ION] BASE DE DATOS ION
  - [E.1] Errores de los usuarios
  - [E.2] Errores del administrador del sistema / de la seguridad
  - [E.15] Alteración de la información
  - [E.18] Destrucción de la información
  - [E.19] Fugas de información
  - [A.5] Suplantación de la identidad
  - [A.6] Abuso de privilegios de acceso
  - [A.11] Acceso no autorizado
  - [A.15] Modificación de la información
  - [A.18] Destrucción de la información
  - [A.19] Revelación de información

ANEXO C

activo	probabilidad	[D]	[I]	[C]
ACTIVOS				
[B] Activos esenciales				
[SCADA_HPA_MAZAR] SCADA ALSPA P320 MAZAR		T	T	T
[N.*.4] Terremotos	MR	T	T	T
[I.2] Daños por agua	MR	T	T	T
[I.*] Desastres industriales	PP	T	T	T
[I.3.3] Polvo	P	A	A	A
[I.5] Avería de origen físico o lógico	P	A	A	A
[I.5.1] Software	P	A	A	A
[I.5.2] Hardware	P	A	A	A
[I.5.3] Equipos de comunicaciones	PP	A	A	A
[I.5.4] Equipamiento auxiliar	PP	A	A	A
[I.6] Corte del suministro eléctrico	PP	A	A	A
[I.7] Condiciones inadecuadas de temperatura o humedad	PP	A	A	A
[I.11] Emanaciones electromagnéticas	PP	A	A	A
[E.2] Errores del administrador del sistema / de la seguridad	P	A	A	A
[E.4] Errores de configuración	P	A	A	A
[E.23] Errores de mantenimiento / actualización de equipos (	P	A	A	A
[E.24] Caída del sistema por agotamiento de recursos	PP	A	A	A
[A.6] Abuso de privilegios de acceso	P	A	A	A
[A.7] Uso no previsto	P	A	A	A
[A.11] Acceso no autorizado	P	A	A	A
[A.23] Manipulación del hardware	PP	A	A	A
[IS] Servicios internos				
[VOIP_TELEF_ IP_HPA_MAZ] TELEFONIA IP		M	M	M
[E.1] Errores de los usuarios	MR	M	M	M
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M
[E.24] Caída del sistema por agotamiento de recursos	P	M	M	M
[A.5] Suplantación de la identidad	PP	M	M	M
[A.7] Uso no previsto	PP	M	M	M
[A.11] Acceso no autorizado	PP	M	M	M
[A.24] Denegación de servicio	PP	M	M	M
[A.28.1] Enfermedad	P	M	M	M
[MOBILE_TELEF_ DECT_HPA_MAZ] TELEFONIA MOVIL		A	A	A
[E.1] Errores de los usuarios	MR	M	M	M
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M
[E.24] Caída del sistema por agotamiento de recursos	P	M	M	M
[A.5] Suplantación de la identidad	PP	A	A	A
[A.7] Uso no previsto	PP	A	A	A
[A.11] Acceso no autorizado	PP	M	M	M
[A.24] Denegación de servicio	PP	A	A	A
[A.28.1] Enfermedad	P	M	M	M
[INT_CCTV_ HPA_MAZ] CCTV VIDEOVIGILANCIA		A	A	A
[E.1] Errores de los usuarios	MR	M	M	M
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M
[E.24] Caída del sistema por agotamiento de recursos	P	M	M	M
[A.5] Suplantación de la identidad	PP	A	A	A
[A.7] Uso no previsto	PP	A	A	A
[A.11] Acceso no autorizado	PP	M	M	M
[A.24] Denegación de servicio	PP	A	A	A
[A.28.1] Enfermedad	P	M	M	M

[WWW_INTERNET_HPA_MAZ] INTERNET		A	A	A	
[E.2] Errores del administrador del sistema / de la seguridad	PP	A	A	A	
[E.24] Caída del sistema por agotamiento de recursos	PP	A	A	A	
[A.7] Uso no previsto	PP	A	A	A	
[A.11] Acceso no autorizado	PP	A	A	A	
[A.24] Denegación de servicio	PP	A	A	A	
[E] Equipamiento					
[SW] Aplicaciones					
[APP_SCADA_HPA_MAZ] SCADA ALSPA P320		A	A	A	
[I.5] Avería de origen físico o lógico	MR	A	A	A	
[E.1] Errores de los usuarios	MR	A	A	A	
[E.2] Errores del administrador del sistema / de la seguri	MR	A	A	A	
[E.8] Difusión de software dañino	MR	A	A	A	
[E.15] Alteración de la información	MR	A	A	A	
[E.18] Destrucción de la información	MR	A	A	A	
[E.19] Fugas de información	MR	A	A	A	
[E.20] Vulnerabilidades de los programas (software)	MR	A	A	A	
[E.21] Errores de mantenimiento / actualización de progr	MR	A	A	A	
[A.5] Suplantación de la identidad	MR	A	A	A	
[A.6] Abuso de privilegios de acceso	MR	A	A	A	
[A.7] Uso no previsto	MR	A	A	A	
[A.8] Difusión de software dañino	MR	A	A	A	
[A.11] Acceso no autorizado	MR	A	A	A	
[A.15] Modificación de la información	MR	A	A	A	
[A.18] Destrucción de la información	MR	A	A	A	
[A.19] Revelación de información	MR	A	A	A	
[A.22] Manipulación de programas	MR	A	A	A	
[SUB_CONTROL CONJUNTO_HPA_MAZ] CONTROL CONJUNT		A	A	A	
[I.5] Avería de origen físico o lógico	MR	A	A	A	
[E.1] Errores de los usuarios	MR	A	A	A	
[E.2] Errores del administrador del sistema / de la seguri	MR	A	A	A	
[E.8] Difusión de software dañino	MR	A	A	A	
[E.15] Alteración de la información	MR	A	A	A	
[E.18] Destrucción de la información	MR	A	A	A	
[E.19] Fugas de información	MR	A	A	A	
[E.20] Vulnerabilidades de los programas (software)	MR	A	A	A	
[E.21] Errores de mantenimiento / actualización de progr	MR	A	A	A	
[A.5] Suplantación de la identidad	MR	A	A	A	
[A.6] Abuso de privilegios de acceso	MR	A	A	A	
[A.7] Uso no previsto	MR	A	A	A	
[A.8] Difusión de software dañino	MR	A	A	A	
[A.11] Acceso no autorizado	MR	A	A	A	
[A.15] Modificación de la información	MR	A	A	A	
[A.18] Destrucción de la información	MR	A	A	A	
[A.19] Revelación de información	MR	A	A	A	
[A.22] Manipulación de programas	MR	A	A	A	

[APP_VIBRACIONES_HPA_MAZ] ZOOM		A	A	A
[I.5] Avería de origen físico o lógico	P	A	A	A
[E.1] Errores de los usuarios	MR	M	M	M
[E.2] Errores del administrador del sistema / de la seguri	P	A	A	A
[E.8] Difusión de software dañino	PP	A	A	A
[E.15] Alteración de la información	PP	A	A	A
[E.18] Destrucción de la información	PP	A	A	A
[E.19] Fugas de información	PP	M	M	M
[E.20] Vulnerabilidades de los programas (software)	PP	A	A	A
[E.21] Errores de mantenimiento / actualización de progr	P	A	A	A
[A.5] Suplantación de la identidad	MR	A	A	A
[A.6] Abuso de privilegios de acceso	P	A	A	A
[A.7] Uso no previsto	MR	A	A	A
[A.8] Difusión de software dañino	PP	A	A	A
[A.11] Acceso no autorizado	P	A	A	A
[A.15] Modificación de la información	PP	A	A	A
[A.18] Destrucción de la información	PP	A	A	A
[A.19] Revelación de información	PP	A	A	A
[A.22] Manipulación de programas	PP	A	A	A
[APP_DES_PARCIALES_HPA_MAZ] DESCARGAS PARCIALES		A	A	A
[I.5] Avería de origen físico o lógico	P	A	A	A
[E.1] Errores de los usuarios	MR	M	M	M
[E.2] Errores del administrador del sistema / de la seguri	P	A	A	A
[E.8] Difusión de software dañino	PP	A	A	A
[E.15] Alteración de la información	PP	A	A	A
[E.18] Destrucción de la información	PP	A	A	A
[E.19] Fugas de información	PP	M	M	M
[E.20] Vulnerabilidades de los programas (software)	PP	A	A	A
[E.21] Errores de mantenimiento / actualización de progr	P	A	A	A
[A.5] Suplantación de la identidad	MR	A	A	A
[A.6] Abuso de privilegios de acceso	P	A	A	A
[A.7] Uso no previsto	MR	A	A	A
[A.8] Difusión de software dañino	PP	A	A	A
[A.11] Acceso no autorizado	P	A	A	A
[A.15] Modificación de la información	PP	A	A	A
[A.18] Destrucción de la información	PP	A	A	A
[A.19] Revelación de información	PP	A	A	A
[A.22] Manipulación de programas	PP	A	A	A

[PRP_AROCHE_HPA_MAZ] AROCHE		A	A	A
[I.5] Avería de origen físico o lógico	P	A	A	A
[I.5.1] Software	P	A	A	A
[E.2] Errores del administrador del sistema / de la seguri	PP	A	A	A
[E.8] Difusión de software dañino	PP	A	A	A
[E.15] Alteración de la información	PP	A	A	A
[E.18] Destrucción de la información	PP	M	M	M
[E.19] Fugas de información	PP	M	M	M
[E.20] Vulnerabilidades de los programas (software)	P	A	A	A
[E.21] Errores de mantenimiento / actualización de progr	P	A	A	A
[A.5] Suplantación de la identidad	PP	M	M	M
[A.6] Abuso de privilegios de acceso	PP	A	A	A
[A.11] Acceso no autorizado	PP	A	A	A
[A.15] Modificación de la información	PP	A	A	A
[A.22] Manipulación de programas	MR	A	A	A
[AV_HPA_MAZ] McAfee		MA	MA	MA
[I.5] Avería de origen físico o lógico	P	MA	MA	MA
[E.1] Errores de los usuarios	MR	M	M	M
[E.2] Errores del administrador del sistema / de la seguri	P	A	A	A
[E.8] Difusión de software dañino	PP	MA	MA	MA
[E.15] Alteración de la información	PP	MA	MA	MA
[E.18] Destrucción de la información	PP	MA	MA	MA
[E.19] Fugas de información	PP	M	M	M
[E.20] Vulnerabilidades de los programas (software)	PP	A	A	A
[E.21] Errores de mantenimiento / actualización de progr	P	MA	MA	MA
[A.5] Suplantación de la identidad	MR	A	A	A
[A.6] Abuso de privilegios de acceso	P	A	A	A
[A.7] Uso no previsto	MR	A	A	A
[A.8] Difusión de software dañino	PP	A	A	A
[A.11] Acceso no autorizado	P	A	A	A
[A.15] Modificación de la información	PP	A	A	A
[A.18] Destrucción de la información	PP	A	A	A
[A.19] Revelación de información	PP	A	A	A
[A.22] Manipulación de programas	PP	MA	MA	MA

[PRP_SCAD_HPA_MAZ] SCAD		A	A	A
[I.5] Avería de origen físico o lógico	P	A	A	A
[I.5.1] Software	P	A	A	A
[E.2] Errores del administrador del sistema / de la seguri	PP	A	A	A
[E.8] Difusión de software dañino	PP	A	A	A
[E.15] Alteración de la información	PP	A	A	A
[E.18] Destrucción de la información	PP	M	M	M
[E.19] Fugas de información	PP	M	M	M
[E.20] Vulnerabilidades de los programas (software)	P	A	A	A
[E.21] Errores de mantenimiento / actualización de progra	P	A	A	A
[A.5] Suplantación de la identidad	PP	M	M	M
[A.6] Abuso de privilegios de acceso	PP	A	A	A
[A.11] Acceso no autorizado	PP	A	A	A
[A.15] Modificación de la información	PP	A	A	A
[A.22] Manipulación de programas	MR	A	A	A
[APP_ION_HPA_MAZ] ION		A	A	A
[I.5] Avería de origen físico o lógico	P	A	A	A
[E.1] Errores de los usuarios	MR	M	M	M
[E.2] Errores del administrador del sistema / de la seguri	P	A	A	A
[E.8] Difusión de software dañino	PP	A	A	A
[E.15] Alteración de la información	PP	A	A	A
[E.18] Destrucción de la información	PP	A	A	A
[E.19] Fugas de información	PP	M	M	M
[E.20] Vulnerabilidades de los programas (software)	PP	A	A	A
[E.21] Errores de mantenimiento / actualización de progra	P	A	A	A
[A.5] Suplantación de la identidad	MR	A	A	A
[A.6] Abuso de privilegios de acceso	P	A	A	A
[A.7] Uso no previsto	MR	A	A	A
[A.8] Difusión de software dañino	PP	A	A	A
[A.11] Acceso no autorizado	P	A	A	A
[A.15] Modificación de la información	PP	A	A	A
[A.18] Destrucción de la información	PP	A	A	A
[A.19] Revelación de información	PP	A	A	A
[A.22] Manipulación de programas	PP	A	A	A
[WINDOWS_HPA_MAZ] WINDOWS		MA	MA	MA
[I.5] Avería de origen físico o lógico	P	MA	MA	MA
[E.2] Errores del administrador del sistema / de la seguri	P	A	A	A
[E.8] Difusión de software dañino	PP	MA	MA	MA
[E.19] Fugas de información	PP	M	M	M
[E.20] Vulnerabilidades de los programas (software)	PP	A	A	A
[E.21] Errores de mantenimiento / actualización de progra	P	MA	MA	MA
[A.6] Abuso de privilegios de acceso	P	A	A	A
[A.7] Uso no previsto	MR	A	A	A
[A.8] Difusión de software dañino	PP	A	A	A
[A.11] Acceso no autorizado	P	A	A	A
[A.22] Manipulación de programas	PP	MA	MA	MA

[STD_CAMPBELL_HPA_MAZ] CAMPBELL LOGGERNET		A	A	A
[I.5] Avería de origen físico o lógico	P	A	A	A
[E.2] Errores del administrador del sistema / de la seguri	PP	M	M	M
[E.8] Difusión de software dañino	PP	A	A	A
[E.19] Fugas de información	PP	A	A	A
[E.20] Vulnerabilidades de los programas (software)	PP	A	A	A
[E.21] Errores de mantenimiento / actualización de progr	P	A	A	A
[A.6] Abuso de privilegios de acceso	PP	A	A	A
[A.7] Uso no previsto	PP	A	A	A
[A.8] Difusión de software dañino	PP	M	M	M
[A.11] Acceso no autorizado	PP	M	M	M
[A.22] Manipulación de programas	MR	M	M	M
[OTHER_GESTIÓN REDES_HPA_MAZ] GESTIÓN REDES		M	M	M
[I.5] Avería de origen físico o lógico	MR	M	M	M
[E.1] Errores de los usuarios	MR	M	M	M
[E.2] Errores del administrador del sistema / de la seguri	MR	M	M	M
[E.8] Difusión de software dañino	MR	M	M	M
[E.15] Alteración de la información	MR	M	M	M
[E.18] Destrucción de la información	MR	M	M	M
[E.19] Fugas de información	MR	M	M	M
[E.20] Vulnerabilidades de los programas (software)	MR	M	M	M
[E.21] Errores de mantenimiento / actualización de progr	MR	M	M	M
[A.5] Suplantación de la identidad	MR	M	M	M
[A.6] Abuso de privilegios de acceso	MR	M	M	M
[A.7] Uso no previsto	MR	M	M	M
[A.8] Difusión de software dañino	MR	M	M	M
[A.11] Acceso no autorizado	MR	M	M	M
[A.15] Modificación de la información	MR	M	M	M
[A.18] Destrucción de la información	MR	M	M	M
[A.19] Revelación de información	MR	M	M	M
[A.22] Manipulación de programas	MR	M	M	M
[HW] Equipos				
[SWITCH_RS20_HPA_MAZ] SWITCH RS20 6TX/FX RED S800		T	T	T
[N.*.4] Terremotos	MR	T	T	T
[I.2] Daños por agua	MR	A	A	A
[I.5.2] Hardware	P	MA	MA	MA
[I.8] Fallo de servicios de comunicaciones	PP	A	A	A
[I.8.11] Interrupción accidental	PP	A	A	A
[E.2] Errores del administrador del sistema / de la seguri	P	A	A	A
[E.4] Errores de configuración	P	MA	MA	MA
[E.9] Errores de [re-]encaminamiento	P	A	A	A
[E.28.1] Enfermedad	P	A	A	A
[SWITCH_RS2_FT802B_HPA_MAZ] SW_OFFICE		T	T	T
[N.*.4] Terremotos	MR	T	T	T
[I.2] Daños por agua	MR	A	A	A
[I.5.2] Hardware	P	MA	MA	MA
[I.8] Fallo de servicios de comunicaciones	PP	A	A	A
[I.8.11] Interrupción accidental	PP	A	A	A
[E.2] Errores del administrador del sistema / de la seguri	P	A	A	A
[E.4] Errores de configuración	P	MA	MA	MA
[E.9] Errores de [re-]encaminamiento	P	A	A	A
[E.28.1] Enfermedad	P	A	A	A

[HOST_PCX_HPA_MAZ] PCX		T	T	T
[N.*.4] Terremotos	MR	T	T	T
[I.2] Daños por agua	PP	MA	MA	MA
[I.3.3] Polvo	P	MA	MA	MA
[I.5.2] Hardware	P	MA	MA	MA
[I.5.3] Equipos de comunicaciones	P	MA	MA	MA
[I.5.4] Equipamiento auxiliar	P	MA	MA	MA
[I.6.11] Interrupción accidental	PP	MA	MA	MA
[I.7] Condiciones inadecuadas de temperatura o humeda	PP	MA	MA	MA
[I.8] Fallo de servicios de comunicaciones	PP	MA	MA	MA
[I.8.11] Interrupción accidental	PP	MA	MA	MA
[I.10] Degradación de los soportes de almacenamiento d	PP	MA	MA	MA
[E.2] Errores del administrador del sistema / de la seguri	PP	MA	MA	MA
[E.4] Errores de configuración	P	MA	MA	MA
[E.9] Errores de [re-]encaminamiento	PP	MA	MA	MA
[E.21] Errores de mantenimiento / actualización de progr	P	MA	MA	MA
[E.23] Errores de mantenimiento / actualización de equip	P	MA	MA	MA
[E.24] Caída del sistema por agotamiento de recursos	PP	MA	MA	MA
[E.28.1] Enfermedad	P	A	A	A
[MID_FC_HPA_MAZ] FC FIELD CONTROLLER		T	T	T
[N.*.4] Terremotos	MR	T	T	T
[I.2] Daños por agua	PP	MA	MA	MA
[I.3.3] Polvo	P	MA	MA	MA
[I.5.2] Hardware	P	MA	MA	MA
[I.5.3] Equipos de comunicaciones	PP	MA	MA	MA
[I.5.4] Equipamiento auxiliar	P	MA	MA	MA
[I.8] Fallo de servicios de comunicaciones	PP	MA	MA	MA
[I.8.11] Interrupción accidental	PP	MA	MA	MA
[I.10] Degradación de los soportes de almacenamiento d	PP	MA	MA	MA
[E.2] Errores del administrador del sistema / de la seguri	PP	MA	MA	MA
[E.4] Errores de configuración	PP	MA	MA	MA
[E.9] Errores de [re-]encaminamiento	PP	MA	MA	MA
[E.21] Errores de mantenimiento / actualización de progr	P	MA	MA	MA
[E.23] Errores de mantenimiento / actualización de equip	P	MA	MA	MA
[E.24] Caída del sistema por agotamiento de recursos	PP	MA	MA	MA
[E.28.1] Enfermedad	P	A	A	A
[MID_IHR_HPA_MAZ] IHR INPUT HIGH RESOLUTION		T	T	T
[N.*.4] Terremotos	MR	T	T	T
[I.2] Daños por agua	PP	MA	MA	MA
[I.3.3] Polvo	P	MA	MA	MA
[I.5.2] Hardware	P	MA	MA	MA
[I.5.3] Equipos de comunicaciones	PP	MA	MA	MA
[I.5.4] Equipamiento auxiliar	P	MA	MA	MA
[I.8] Fallo de servicios de comunicaciones	PP	MA	MA	MA
[I.8.11] Interrupción accidental	PP	MA	MA	MA
[I.10] Degradación de los soportes de almacenamiento d	PP	MA	MA	MA
[E.2] Errores del administrador del sistema / de la seguri	PP	MA	MA	MA
[E.4] Errores de configuración	PP	MA	MA	MA
[E.9] Errores de [re-]encaminamiento	PP	MA	MA	MA
[E.21] Errores de mantenimiento / actualización de progr	P	MA	MA	MA
[E.23] Errores de mantenimiento / actualización de equip	P	MA	MA	MA
[E.24] Caída del sistema por agotamiento de recursos	PP	MA	MA	MA
[E.28.1] Enfermedad	P	A	A	A
[OTHER_GPS-01-ES_HPA_MAZ] GPS-01		MA	MA	MA
[N.*.4] Terremotos	MA	MA	MA	MA
[I.2] Daños por agua	PP	A	A	A
[I.8] Fallo de servicios de comunicaciones	PP	M	M	M
[I.8.11] Interrupción accidental	PP	M	M	M
[E.2] Errores del administrador del sistema / de la seguri	P	M	M	M

[OTHER_M_FOX_515_HPA_MAZ] MULTIPLEXOR X 515		A	A	A
[N.*.4] Terremotos	MR	A	A	A
[I.1] Fuego	MR	A	A	A
[I.2] Daños por agua	MR	A	A	A
[I.3] Contaminación medioambiental	P	M	M	M
[I.3.3] Polvo	P	M	M	M
[I.5] Avería de origen físico o lógico	P	A	A	A
[I.5.1] Software	P	A	A	A
[I.5.2] Hardware	P	A	A	A
[I.5.3] Equipos de comunicaciones	PP	M	M	M
[I.6] Corte del suministro eléctrico	PP	B	B	B
[I.6.11] Interrupción accidental	PP	B	B	B
[I.7] Condiciones inadecuadas de temperatura o humeda	PP	M	M	M
[I.8] Fallo de servicios de comunicaciones	MR	B	B	B
[I.8.11] Interrupción accidental	PP	B	B	B
[I.11] Emanaciones electromagnéticas	PP	B	B	B
[I.11.1] Radio	PP	B	B	B
[E] Errores y fallos no intencionados	PP	B	B	B
[E.2] Errores del administrador del sistema / de la seguri	PP	M	M	M
[E.4] Errores de configuración	P	M	M	M
[E.9] Errores de [re-]encaminamiento	PP	M	M	M
[E.10] Errores de secuencia	P	M	M	M
[E.14] Fugas de información (> E.19)	PP	M	M	M
[E.19] Fugas de información	PP	M	M	M
[E.19.1] A personal interno que no necesita conocerlo	PP	M	M	M
[E.21] Errores de mantenimiento / actualización de progr	P	M	M	M
[E.23] Errores de mantenimiento / actualización de equip	P	M	M	M
[E.24] Caída del sistema por agotamiento de recursos	P	A	A	A
[E.28] Indisponibilidad del personal	P	M	M	M
[E.28.1] Enfermedad	P	A	A	A
[A.4] Manipulación de los ficheros de configuración	PP	A	A	A
[A.5] Suplantación de la identidad	MR	M	M	M
[A.5.1] Por personal interno	MR	M	M	M
[A.6] Abuso de privilegios de acceso	MR	M	M	M
[A.6.1] Por personal interno	MR	M	M	M
[A.11] Acceso no autorizado	MR	A	A	A
[A.11.1] Por personal interno	MR	A	A	A
[A.19] Revelación de información	MR	M	M	M
[A.19.1] A personal interno que no necesita conocerlo	MR	M	M	M
[A.28] Indisponibilidad del personal	P	A	A	A
[A.28.1] Enfermedad	P	A	A	A

[OTHER_M_UMUX_1500_HPA_MAZ] MULTIPLEXOR UMUX 15		A	A	A
[N.*.4] Terremotos	MR	A	A	A
[I.1] Fuego	MR	A	A	A
[I.2] Daños por agua	MR	A	A	A
[I.3] Contaminación medioambiental	P	M	M	M
[I.3.3] Polvo	P	M	M	M
[I.5] Avería de origen físico o lógico	P	A	A	A
[I.5.1] Software	P	A	A	A
[I.5.2] Hardware	P	A	A	A
[I.5.3] Equipos de comunicaciones	PP	M	M	M
[I.6] Corte del suministro eléctrico	PP	B	B	B
[I.6.11] Interrupción accidental	PP	B	B	B
[I.7] Condiciones inadecuadas de temperatura o humeda	PP	M	M	M
[I.8] Fallo de servicios de comunicaciones	MR	B	B	B
[I.8.11] Interrupción accidental	PP	B	B	B
[I.11] Emanaciones electromagnéticas	PP	B	B	B
[I.11.1] Radio	PP	B	B	B
[E] Errores y fallos no intencionados	PP	B	B	B
[E.2] Errores del administrador del sistema / de la seguri	PP	M	M	M
[E.4] Errores de configuración	P	M	M	M
[E.9] Errores de [re-]encaminamiento	PP	M	M	M
[E.10] Errores de secuencia	P	M	M	M
[E.14] Fugas de información (> E.19)	PP	M	M	M
[E.19] Fugas de información	PP	M	M	M
[E.19.1] A personal interno que no necesita conocerlo	PP	M	M	M
[E.21] Errores de mantenimiento / actualización de progra	P	M	M	M
[E.23] Errores de mantenimiento / actualización de equip	P	M	M	M
[E.24] Caída del sistema por agotamiento de recursos	P	A	A	A
[E.28] Indisponibilidad del personal	P	M	M	M
[E.28.1] Enfermedad	P	A	A	A
[A.4] Manipulación de los ficheros de configuración	PP	A	A	A
[A.5] Suplantación de la identidad	MR	M	M	M
[A.5.1] Por personal interno	MR	M	M	M
[A.6] Abuso de privilegios de acceso	MR	M	M	M
[A.6.1] Por personal interno	MR	M	M	M
[A.11] Acceso no autorizado	MR	A	A	A
[A.11.1] Por personal interno	MR	A	A	A
[A.19] Revelación de información	MR	M	M	M
[A.19.1] A personal interno que no necesita conocerlo	MR	M	M	M
[A.28] Indisponibilidad del personal	P	A	A	A
[A.28.1] Enfermedad	P	A	A	A
[MID_C30_1-3-4_HPA_MAZ] CONSOLA CIS/CVS 1-3-4 MAZAR		T	T	T
[N.*.4] Terremotos	MR	T	T	T
[I.3.3] Polvo	P	A	A	A
[I.5.1] Software	P	A	A	A
[I.5.2] Hardware	P	A	A	A
[I.5.3] Equipos de comunicaciones	PP	M	M	M
[I.5.4] Equipamiento auxiliar	MR	M	M	M
[I.6.11] Interrupción accidental	MR	M	M	M
[I.8] Fallo de servicios de comunicaciones	MR	M	M	M
[I.8.11] Interrupción accidental	MR	A	A	A
[E.2] Errores del administrador del sistema / de la seguri	PP	A	A	A
[E.9] Errores de [re-]encaminamiento	PP	M	M	M
[E.21] Errores de mantenimiento / actualización de progra	P	A	A	A
[E.23] Errores de mantenimiento / actualización de equip	P	A	A	A
[E.24] Caída del sistema por agotamiento de recursos	PP	A	A	A
[E.28.1] Enfermedad	P	A	A	A
[A.8.1] Virus	P	A	A	A
[A.11.1] Por personal interno	P	A	A	A
[A.22.5] Autenticación débil	P	A	A	A
[A.22.6] Se elude la autenticación	P	A	A	A

[MID_CCC_HPA_MAZ] CONSOLA CCC MAZAR-MOLINO		T	T	T
[N.*.4] Terremotos	MR	T	T	T
[I.3.3] Polvo	P	A	A	A
[I.5.1] Software	P	A	A	A
[I.5.2] Hardware	P	A	A	A
[I.5.3] Equipos de comunicaciones	PP	M	M	M
[I.5.4] Equipamiento auxiliar	MR	M	M	M
[I.6.11] Interrupción accidental	MR	M	M	M
[I.8] Fallo de servicios de comunicaciones	MR	M	M	M
[I.8.11] Interrupción accidental	MR	A	A	A
[E.2] Errores del administrador del sistema / de la seguri	PP	A	A	A
[E.9] Errores de [re-]encaminamiento	PP	M	M	M
[E.21] Errores de mantenimiento / actualización de progra	P	A	A	A
[E.23] Errores de mantenimiento / actualización de equip	P	A	A	A
[E.24] Caída del sistema por agotamiento de recursos	PP	A	A	A
[E.28.1] Enfermedad	P	A	A	A
[A.8.1] Virus	P	A	A	A
[A.11.1] Por personal interno	P	A	A	A
[A.22.5] Autenticación débil	P	A	A	A
[A.22.6] Se elude la autenticación	P	A	A	A
[MID_CONTROCAD_HPA_MAZ] CONTROCAD SERVER MAZAR		T	T	T
[N.*.4] Terremotos	MR	T	T	T
[I.3.3] Polvo	P	A	A	A
[I.5.1] Software	P	A	A	A
[I.5.2] Hardware	P	A	A	A
[I.5.3] Equipos de comunicaciones	PP	M	M	M
[I.5.4] Equipamiento auxiliar	MR	M	M	M
[I.6.11] Interrupción accidental	MR	M	M	M
[I.8] Fallo de servicios de comunicaciones	MR	M	M	M
[I.8.11] Interrupción accidental	MR	A	A	A
[E.2] Errores del administrador del sistema / de la seguri	PP	A	A	A
[E.9] Errores de [re-]encaminamiento	PP	M	M	M
[E.21] Errores de mantenimiento / actualización de progra	P	A	A	A
[E.23] Errores de mantenimiento / actualización de equip	P	A	A	A
[E.24] Caída del sistema por agotamiento de recursos	PP	A	A	A
[E.28.1] Enfermedad	P	A	A	A
[A.8.1] Virus	P	A	A	A
[A.11.1] Por personal interno	P	A	A	A
[A.22.5] Autenticación débil	P	A	A	A
[A.22.6] Se elude la autenticación	P	A	A	A
[MID_C10_HPA_MAZ] CONSOLA C10		T	T	T
[N.*.4] Terremotos	MR	T	T	T
[I.3.3] Polvo	P	A	A	A
[I.5.1] Software	P	A	A	A
[I.5.2] Hardware	P	A	A	A
[I.5.3] Equipos de comunicaciones	PP	M	M	M
[I.5.4] Equipamiento auxiliar	MR	M	M	M
[I.6.11] Interrupción accidental	MR	M	M	M
[I.8] Fallo de servicios de comunicaciones	MR	M	M	M
[I.8.11] Interrupción accidental	MR	A	A	A
[E.2] Errores del administrador del sistema / de la seguri	PP	A	A	A
[E.9] Errores de [re-]encaminamiento	PP	M	M	M
[E.21] Errores de mantenimiento / actualización de progra	P	A	A	A
[E.23] Errores de mantenimiento / actualización de equip	P	A	A	A
[E.24] Caída del sistema por agotamiento de recursos	PP	A	A	A
[E.28.1] Enfermedad	P	A	A	A
[A.8.1] Virus	P	A	A	A
[A.11.1] Por personal interno	P	A	A	A
[A.22.5] Autenticación débil	P	A	A	A
[A.22.6] Se elude la autenticación	P	A	A	A

[PC_HPA_MAZ] SCAD-AROCHE-ION-PROTECCIONES-DATOS(		T	T	T
[N.*.4] Terremotos	MR	T	T	T
[I.3.3] Polvo	P	A	A	A
[I.5.1] Software	P	A	A	A
[I.5.2] Hardware	P	A	A	A
[I.5.3] Equipos de comunicaciones	PP	M	M	M
[I.5.4] Equipamiento auxiliar	MR	M	M	M
[I.6.11] Interrupción accidental	MR	M	M	M
[I.8] Fallo de servicios de comunicaciones	MR	M	M	M
[I.8.11] Interrupción accidental	MR	A	A	A
[E.2] Errores del administrador del sistema / de la seguri	PP	A	A	A
[E.9] Errores de [re-]encaminamiento	PP	M	M	M
[E.21] Errores de mantenimiento / actualización de progr	P	A	A	A
[E.23] Errores de mantenimiento / actualización de equip	P	A	A	A
[E.24] Caída del sistema por agotamiento de recursos	PP	A	A	A
[E.28.1] Enfermedad	P	A	A	A
[A.8.1] Virus	P	A	A	A
[A.11.1] Por personal interno	P	A	A	A
[A.22.5] Autenticación débil	P	A	A	A
[A.22.6] Se elude la autenticación	P	A	A	A
[DATA_VIBRACIONES_HPA_MAZ] VIBRACIONES_SERVER		T	T	T
[N.*.4] Terremotos	MR	T	T	T
[I.3.3] Polvo	P	A	A	A
[I.5.1] Software	P	A	A	A
[I.5.2] Hardware	P	A	A	A
[I.5.3] Equipos de comunicaciones	PP	M	M	M
[I.5.4] Equipamiento auxiliar	MR	M	M	M
[I.6.11] Interrupción accidental	MR	M	M	M
[I.8] Fallo de servicios de comunicaciones	MR	M	M	M
[I.8.11] Interrupción accidental	MR	A	A	A
[E.2] Errores del administrador del sistema / de la seguri	PP	A	A	A
[E.9] Errores de [re-]encaminamiento	PP	M	M	M
[E.21] Errores de mantenimiento / actualización de progr	P	A	A	A
[E.23] Errores de mantenimiento / actualización de equip	P	A	A	A
[E.24] Caída del sistema por agotamiento de recursos	PP	A	A	A
[E.28.1] Enfermedad	P	A	A	A
[A.8.1] Virus	P	A	A	A
[A.11.1] Por personal interno	P	A	A	A
[A.22.5] Autenticación débil	P	A	A	A
[A.22.6] Se elude la autenticación	P	A	A	A
[COM] Comunicaciones				
[COM_RED S8000] RED S8000-1/2		T	T	T
[N.*.4] Terremotos	MR	T	T	T
[I.8] Fallo de servicios de comunicaciones	P	MA	MA	MA
[I.8.11] Interrupción accidental	PP	MA	MA	MA
[E.2] Errores del administrador del sistema / de la seguri	P	A	A	A
[E.9] Errores de [re-]encaminamiento	P	A	A	A
[E.28.1] Enfermedad	P	A	A	A

[COM_RED F8000-1/2] RED F8000-1/2		T	T	T
[N.*.4] Terremotos	MR	T	T	T
[I.8] Fallo de servicios de comunicaciones	PP	MA	MA	MA
[I.8.11] Interrupción accidental	PP	MA	MA	MA
[E.2] Errores del administrador del sistema / de la seguri	P	A	A	A
[E.9] Errores de [re-]encaminamiento	P	A	A	A
[E.28.1] Enfermedad	P	A	A	A
[COM_RED OFFICE] RED OFFICE		T	T	T
[N.*.4] Terremotos	MR	T	T	T
[I.8] Fallo de servicios de comunicaciones	P	MA	MA	MA
[I.8.11] Interrupción accidental	PP	MA	MA	MA
[E.2] Errores del administrador del sistema / de la seguri	P	A	A	A
[E.9] Errores de [re-]encaminamiento	P	A	A	A
[E.28.1] Enfermedad	P	A	A	A
[COM_LAN] RED LAN		MA	MA	MA
[I.8] Fallo de servicios de comunicaciones	PP	MA	MA	MA
[E.2] Errores del administrador del sistema / de la seguri	PP	A	A	A
[E.9] Errores de [re-]encaminamiento	PP	A	A	A
[E.10] Errores de secuencia	PP	A	A	A
[E.15] Alteración de la información	PP	A	A	A
[E.19] Fugas de información	PP	A	A	A
[E.24] Caida del sistema por agotamiento de recursos	P	A	A	A
[A.7] Uso no previsto	PP	M	M	M
[A.9] [Re-]encaminamiento de mensajes	PP	M	M	M
[A.11] Acceso no autorizado	PP	A	A	A
[A.12] Análisis de tráfico	PP	A	A	A
[A.14] Interceptación de información (escucha)	PP	A	A	A
[A.24] Denegación de servicio	PP	A	A	A
[PABX_TELEF_HPA_MAZ] CENTRAL TELEFONICA MAZAR		A	A	A
[I.2] Daños por agua	PP	A	A	A
[I.*] Desastres industriales	PP	A	A	A
[I.3] Contaminación medioambiental	P	M	M	M
[I.3.3] Polvo	P	M	M	M
[I.5] Avería de origen físico o lógico	P	A	A	A
[I.6] Corte del suministro eléctrico	PP	A	A	A
[I.7] Condiciones inadecuadas de temperatura o humeda	PP	M	M	M
[I.8] Fallo de servicios de comunicaciones	PP	A	A	A
[E.2] Errores del administrador del sistema / de la seguri	PP	A	A	A
[E.9] Errores de [re-]encaminamiento	PP	M	M	M
[E.10] Errores de secuencia	PP	M	M	M
[E.15] Alteración de la información	PP	A	A	A
[E.19] Fugas de información	PP	A	A	A
[E.23] Errores de mantenimiento / actualización de equip	PP	A	A	A
[E.24] Caída del sistema por agotamiento de recursos	P	A	A	A
[A.23] Manipulación del hardware	PP	A	A	A
[A.24] Denegación de servicio	PP	A	A	A
[Media] Soportes de información				
[DVD_HPA_MAZ] INSTALADORES SCADA ALSPA P320		M	M	M
[I.*] Desastres industriales	PP	M	M	M
[I.5] Avería de origen físico o lógico	P	M	M	M
[E.25] Pérdida de equipos	PP	M	M	M
[A.11] Acceso no autorizado	PP	M	M	M
[A.18] Destrucción de la información	PP	M	M	M
[A.23] Manipulación del hardware	PP	M	M	M

[D] Datos						
[FILES_HISTORIAN] BASE DE DATOS			MA	MA	MA
[E.1] Errores de los usuarios		MR	MA	MA	MA
[E.2] Errores del administrador del sistema / de la seguridad		PP	MA	MA	MA
[E.15] Alteración de la información		PP	MA	MA	MA
[E.18] Destrucción de la información		PP	MA	MA	MA
[E.19] Fugas de información		PP	MA	MA	MA
[A.5] Suplantación de la identidad		PP	MA	MA	MA
[A.6] Abuso de privilegios de acceso		PP	MA	MA	MA
[A.11] Acceso no autorizado		PP	MA	MA	MA
[A.15] Modificación de la información		PP	MA	MA	MA
[A.18] Destrucción de la información		PP	MA	MA	MA
[A.19] Revelación de información		PP	MA	MA	MA
[FILES_SCAD] BASE DE DATOS SCAD			MA	MA	MA
[E.1] Errores de los usuarios		MR	MA	MA	MA
[E.2] Errores del administrador del sistema / de la seguridad		PP	MA	MA	MA
[E.15] Alteración de la información		PP	MA	MA	MA
[E.18] Destrucción de la información		PP	MA	MA	MA
[E.19] Fugas de información		PP	MA	MA	MA
[A.5] Suplantación de la identidad		PP	MA	MA	MA
[A.6] Abuso de privilegios de acceso		PP	MA	MA	MA
[A.11] Acceso no autorizado		PP	MA	MA	MA
[A.15] Modificación de la información		PP	MA	MA	MA
[A.18] Destrucción de la información		PP	MA	MA	MA
[A.19] Revelación de información		PP	MA	MA	MA
[FILES_AROCHE] BASE DE DATOS AROCHE			MA	MA	MA
[E.1] Errores de los usuarios		MR	MA	MA	MA
[E.2] Errores del administrador del sistema / de la seguridad		PP	MA	MA	MA
[E.15] Alteración de la información		PP	MA	MA	MA
[E.18] Destrucción de la información		PP	MA	MA	MA
[E.19] Fugas de información		PP	MA	MA	MA
[A.5] Suplantación de la identidad		PP	MA	MA	MA
[A.6] Abuso de privilegios de acceso		PP	MA	MA	MA
[A.11] Acceso no autorizado		PP	MA	MA	MA
[A.15] Modificación de la información		PP	MA	MA	MA
[A.18] Destrucción de la información		PP	MA	MA	MA
[A.19] Revelación de información		PP	MA	MA	MA
[FILES_VIBRACIONES_HPA_MAZ] ZOOM			MA	MA	MA
[E.1] Errores de los usuarios		MR	MA	MA	MA
[E.2] Errores del administrador del sistema / de la seguridad		PP	MA	MA	MA
[E.15] Alteración de la información		PP	MA	MA	MA
[E.18] Destrucción de la información		PP	MA	MA	MA
[E.19] Fugas de información		PP	MA	MA	MA
[A.5] Suplantación de la identidad		PP	MA	MA	MA
[A.6] Abuso de privilegios de acceso		PP	MA	MA	MA
[A.11] Acceso no autorizado		PP	MA	MA	MA
[A.15] Modificación de la información		PP	MA	MA	MA
[A.18] Destrucción de la información		PP	MA	MA	MA
[A.19] Revelación de información		PP	MA	MA	MA

[FILES_ARGIS] BASE DE DATOS PROTECCIONES ARGIS		MA	MA	MA
[E.1] Errores de los usuarios	MR	MA	MA	MA
[E.2] Errores del administrador del sistema / de la seguridad	PP	MA	MA	MA
[E.15] Alteración de la información	PP	MA	MA	MA
[E.18] Destrucción de la información	PP	MA	MA	MA
[E.19] Fugas de información	PP	MA	MA	MA
[A.5] Suplantación de la identidad	PP	MA	MA	MA
[A.6] Abuso de privilegios de acceso	PP	MA	MA	MA
[A.11] Acceso no autorizado	PP	MA	MA	MA
[A.15] Modificación de la información	PP	MA	MA	MA
[A.18] Destrucción de la información	PP	MA	MA	MA
[A.19] Revelación de información	PP	MA	MA	MA
[FILES_DESCARGASPARCIALES_HPA_MAZ] DESCARGASPARCIA		MA	MA	MA
[E.1] Errores de los usuarios	MR	MA	MA	MA
[E.2] Errores del administrador del sistema / de la seguridad	PP	MA	MA	MA
[E.15] Alteración de la información	PP	MA	MA	MA
[E.18] Destrucción de la información	PP	MA	MA	MA
[E.19] Fugas de información	PP	MA	MA	MA
[A.5] Suplantación de la identidad	PP	MA	MA	MA
[A.6] Abuso de privilegios de acceso	PP	MA	MA	MA
[A.11] Acceso no autorizado	PP	MA	MA	MA
[A.15] Modificación de la información	PP	MA	MA	MA
[A.18] Destrucción de la información	PP	MA	MA	MA
[A.19] Revelación de información	PP	MA	MA	MA
[FILES_LOGGERNET] BASE DE DATOS LOGGERNET		MA	MA	MA
[E.1] Errores de los usuarios	MR	MA	MA	MA
[E.2] Errores del administrador del sistema / de la seguridad	PP	MA	MA	MA
[E.15] Alteración de la información	PP	MA	MA	MA
[E.18] Destrucción de la información	PP	MA	MA	MA
[E.19] Fugas de información	PP	MA	MA	MA
[A.5] Suplantación de la identidad	PP	MA	MA	MA
[A.6] Abuso de privilegios de acceso	PP	MA	MA	MA
[A.11] Acceso no autorizado	PP	MA	MA	MA
[A.15] Modificación de la información	PP	MA	MA	MA
[A.18] Destrucción de la información	PP	MA	MA	MA
[A.19] Revelación de información	PP	MA	MA	MA
[FILES_ION] BASE DE DATOS ION		MA	MA	MA
[E.1] Errores de los usuarios	MR	MA	MA	MA
[E.2] Errores del administrador del sistema / de la seguridad	PP	MA	MA	MA
[E.15] Alteración de la información	PP	MA	MA	MA
[E.18] Destrucción de la información	PP	MA	MA	MA
[E.19] Fugas de información	PP	MA	MA	MA
[A.5] Suplantación de la identidad	PP	MA	MA	MA
[A.6] Abuso de privilegios de acceso	PP	MA	MA	MA
[A.11] Acceso no autorizado	PP	MA	MA	MA
[A.15] Modificación de la información	PP	MA	MA	MA
[A.18] Destrucción de la información	PP	MA	MA	MA
[A.19] Revelación de información	PP	MA	MA	MA

ANEXO D

RESUMEN DEL ESTADO DE LA CONTINGENCIA

Identificación: Colaborador | Almacenamiento: Impreso/Digital| Archivo activo: Mientras el colaborador este activo | Retención: TIC |Vigencia: dia/mes/año | Versión: 1.0

INFORMACIÓN DEL INCIDENTE Y DE LA PERSONA QUE REPORTA			
CÓDIGO			
TIPO DE INCIDENTE		**LUGAR DEL INCIDENTE :**	
NOMBRE DE QUIÉN REPORTA :		**FUNCIONARIO DE QUE EMPRESA Ó CIUDADANO:**	

ACTIVIDAD	PROCEDIMIENTO APLICADO	RESULTADO/ESTADO	FECHA Y HORA	

FIRMA

ANEXO E

PROCEDIMIENTO PARA RECUPERACIÓN

Identificación: Colaborador | Almacenamiento: Impreso/Digital| Archivo activo: Mientras el colaborador este activo | Retención: TIC |Vigencia: dia/mes/año | Versión: 1.0

INFORMACIÓN RELEVANTE	
CÓDIGO	PCI-PR01
NOMBRE CONTINGENCIA	Incendio
FUENTES DE RIESGO	**ESTIMACIÓN DE RIESGO**
Hardware Software Equipos auxiliares Instalaciones	Alto

EQUIPO DE RECUPERACIÓN	
NOMBRE DEL EQUIPO :	Soluciones Producción Mazar SPMZ

LIDER DEL EQUIPO	
PRINCIPAL	Ing. Jaime Matute
SUPLENTE	Ing. Geovanny Dominguez / Ing. Lenin Andrade

MIEMBROS DEL EQUIPO		
	PRINCIPAL	**SUPLENTE**
1	Ing. Jaime Matute Analista de Soluciones Administrativas	Ing. Geovanny Dominguez Asistente SPMZ
2	Ing. Geovanny Dominguez Asistente SPMZ	Ing. Lenin Andrade Asistente SPMZ
3	Ing. Lenin Andrade Asistente SPMZ	

1. Luego del aviso de activación del plan por parte del CPCI
2. Lider solicita al Jefe de Operación aplicar el plan de evacuación (de ser posible) del hardware
3. Lider SPMZ y Asistente de SPMAZ acuden a centro de control alterno.
4. Lider SPMZ y Asistente de SPMAZ confirma operatividad de la C30 alterno
5. Lider SPMZ solicita a Jefe de Operación enviar a personal de Operación al centro de control Alterno.
6. Operadores de centro de control acceden a operar las máquinas de generación desde el sitio alterno
7. Lider SPMZ informa de normalización del control y supervición desde sitio alterno a Jefe de Operación y CPCI

CPCI= Coordinador del Plan Contingencia Informática
SPMZ= Equipo de Soluciones de Producción Mazar
C30= Central Log Alterno (Servidores CIS 1 y CIS2 para operar y supervisar unidades de generación)

PROCEDIMIENTO PARA RECUPERACIÓN

Identificación: Colaborador | Almacenamiento: Impreso/Digital| Archivo activo: Mientras el colaborador este activo | Retención: TIC |Vigencia: dia/mes/año | Versión: 1.0

INFORMACIÓN RELEVANTE	
CÓDIGO	PCI-PR02
NOMBRE CONTINGENCIA	Inundación
FUENTES DE RIESGO	**ESTIMACIÓN DE RIESGO**
Hardware Software Equipos auxiliares Instalaciones	Alto

EQUIPO DE RECUPERACIÓN	
NOMBRE DEL EQUIPO :	Soluciones Producción Mazar SPMZ

LIDER DEL EQUIPO	
PRINCIPAL	Ing. Jaime Matute
SUPLENTE	Ing. Geovanny Dominguez / Ing. Lenin Andrade

MIEMBROS DEL EQUIPO		
	PRINCIPAL	**SUPLENTE**
1	Ing. Jaime Matute Analista de Soluciones	Ing. Geovanny Dominguez Asistente SPMZ
2	Ing. Geovanny Dominguez Asistente SPMZ	Ing. Lenin Andrade Asistente SPMZ
3	Ing. Lenin Andrade Asistente SPMZ	

1. Luego del aviso de activación del plan por parte del CPCI
2. Lider solicita al Jefe de Operación aplicar el plan de evacuación (de ser posible) del hardware
3. Lider SPMZ y Asistente de SPMAZ acuden a centro de control alterno.
4. Lider SPMZ y Asistente de SPMAZ confirma operatividad de la C30 alterno
5. Lider SPMZ solicita a Jefe de Operación enviar a personal de Operación al centro de control Alterno.
6. Operadores de centro de control acceden a operar las máquinas de generación desde el sitio alterno
7. Lider SPMZ informa de normalización del control y supervición desde sitio alterno a Jefe de Operación y CPCI

CPCI= Coordinador del Plan Contingencia Informática
SPMZ= Equipo de Soluciones de Producción Mazar
C30= Central Log Alterno (Servidores CIS 1 y CIS2 para operar y supervisar unidades de generación)

PROCEDIMIENTO PARA RECUPERACIÓN

Identificación: Colaborador | Almacenamiento: Impreso/Digital| Archivo activo: Mientras el colaborador este activo | Retención: TIC |Vigencia: dia/mes/año | Versión: 1.0

INFORMACIÓN RELEVANTE	
CÓDIGO	PCI-PR03
NOMBRE CONTINGENCIA	Falta de suministro eléctrico
FUENTES DE RIESGO	**ESTIMACIÓN DE RIESGO**
Hardware Software Equipos auxiliares	Alto

EQUIPO DE RECUPERACIÓN	
NOMBRE DEL EQUIPO :	Soluciones Producción Mazar SPMZ

LIDER DEL EQUIPO	
PRINCIPAL	Ing. Jaime Matute
SUPLENTE	Ing. Geovanny Dominguez / Ing. Lenin Andrade

MIEMBROS DEL EQUIPO		
	PRINCIPAL	**SUPLENTE**
1	Ing. Jaime Matute Analista de Soluciones Administrativas	Ing. Geovanny Dominguez Asistente SPMZ
2	Ing. Geovanny Dominguez Asistente SPMZ	Ing. Lenin Andrade Asistente SPMZ
3	Ing. Lenin Andrade Asistente SPMZ	

1. Luego del aviso de activación del plan por parte del CPCI
2. Lider SPMZ y Asistente de SPMAZ acuden a centro de control alterno.
3. Lider SPMZ y Asistente de SPMAZ confirma operatividad de la C30 alterno
4. Lider SPMZ solicita a Jefe de Operación enviar a personal de Operación al centro de control Alterno.
5. Operadores de centro de control acceden a operar las máquinas de generación desde el sitio alterno
6. Lider SPMZ informa de normalización del control y supervición desde sitio alterno a Jefe de Operación y CPCI

OBSERVACIONES
CPCI= Coordinador del Plan Contingencia Informática **SPMZ= Equipo de Soluciones de Producción Mazar** **C30= Central Log Alterno (Servidores CIS 1 y CIS2 para operar y supervisar unidades de generación)**

PROCEDIMIENTO PARA RECUPERACIÓN

Identificación: Colaborador | Almacenamiento: Impreso/Digital| Archivo activo: Mientras el colaborador este activo | Retención: TIC |Vigencia: dia/mes/año | Versión: 1.0

INFORMACIÓN RELEVANTE	
CÓDIGO	PCI-PR04
NOMBRE CONTINGENCIA	Indisponibilidad C30 - CCC - CCAD
FUENTES DE RIESGO	**ESTIMACIÓN DE RIESGO**
Hardware	Alto

EQUIPO DE RECUPERACIÓN	
NOMBRE DEL EQUIPO :	Soluciones Producción Mazar SPMZ

LIDER DEL EQUIPO	
PRINCIPAL	Ing. Jaime Matute
SUPLENTE	Ing. Geovanny Dominguez / Ing. Lenin Andrade

MIEMBROS DEL EQUIPO

	PRINCIPAL	SUPLENTE
1	Ing. Jaime Matute Analista de Soluciones Administrativas	Ing. Geovanny Dominguez Asistente SPMZ
2	Ing. Geovanny Dominguez Asistente SPMZ	Ing. Lenin Andrade Asistente SPMZ
3	Ing. Lenin Andrade Asistente SPMZ	

ACCIONES

1. Luego del aviso de activación del plan por parte del CPCI
2. Lider SPMZ comunica Asistente SPMZ para que realice las gestiones pertinentes con asistente de bodega y retire las C30 CCC y CCAD de repuesto para llevarlos a la planta de generación. Además de llevar el respaldo de la imagen con la última configuración de los
3. Lider SPMZ y Asistente de SPMZ analizan causa del fallo de los equipos.
4. Lider SPMZ y Asistente de SPMZ desenergizan los equipos.
5. Lider SPMZ y Asistente de SPMZ proceden a remplazar los equipos.
6. Lider SPMZ y Asistente de SPMZ energizan los equipos.
7. Lider SPMZ y Asistente de SPMZ proceden a restaurar la última imagen de respaldo de
8. Lider SPMZ y Analista de SPMZ realizan pruebas de funcionamiento y operatividad de los e
9. Lider SPMZ informa de la recuperación y operatividad de las PCX a Jefe de Operación y CP

OBSERVACIONES

CPCI= Coordinador del Plan Contingencia Informática
SPMZ= Equipo de Soluciones de Producción Mazar
C30= Cell Control log CIS 1 , CIS 2 y C10
CCC = Centro de Configuración
CCAD= Centro de Arquitectura

DETALLES RECUPERACIÓN HARDWARE Y SOFTWARE
PRI-PR04.1 C30 CCC CCAD

PROCEDIMIENTO PARA RECUPERACIÓN

Identificación: Colaborador | Almacenamiento: Impreso/Digital| Archivo activo: Mientras el colaborador este activo | Retención: TIC |Vigencia: dia/mes/año | Versión: 1.0

INFORMACIÓN RELEVANTE						
CÓDIGO	PCI-PR04.1					
NOMBRE DEL HARDWARE:	C30 CCC CCAD					
OBJETIVOS:	Documentar el procedimiento de restauración de C30 - CCC - CCAD					
DISTRIBUCIÓN:	Ing. Jaime Matute Ing. Geovanny Dominguez Ing. Lenin Andrade					
TMI (RTO)	4 Horas					
EQUIPO DE RECUPERACIÓN						
NOMBRE DEL EQUIPO :	Soluciones de Producción Mazar (SPMZ)					
LIDER DEL EQUIPO						
PRINCIPAL	Ing. Jaime Matute					
SUPLENTE	Ing. Geovanny Dominguez / Ing. Lenin Andrade					
MIEMBROS DEL EQUIPO						
	PRINCIPAL			**ALTERNO**		
1	Ing. Jaime Matute Analista de Soluciones Administrativas			Ing. Geovanny Dominguez Asistente SPMZ		
2	Ing. Geovanny Dominguez Asistente SPMZ			Ing. Lenin Andrade Asistente SPMZ		
3	Ing. Lenin Andrade Asistente SPMZ					
DETALLES DEL HARDWARE						
MARCA/MODELO	Dell™ OptiPlex™ 745 32 bits					
PROCESADORES	Intel® Core™ 2 Duo 1066MHz FSB Socket T with Dual Core technology XD, EM64T, 2MB and up to 4MB L2 cache, EIST and VT (E6000 series)					
SISTEMA OPERATIVO	Microsoft® Windows® XP Professional	**VERSIÓN**	SP2	**ACTUALIZACIÓN**	N/A	
BASE DATOS	N/A	**VERSIÓN**	N/A	**ACTUALIZACIÓN**	N/A	
FUENTE DE PODER	CANTIDAD	1				
	MODELO	DELL				
	POTENCIA	305W				
	VOLTAJE	90 to 135 V at 50/60 Hz; 180 to 265 V at 50/60 Hz				
DISCOS DUROS	CANTIDAD	2				
	DESCRIPCIÓN	Serial ATA or Serial ATA 3.0 7200RPM SATA 3.0Gb/s:160GB				
INPUT/OUTPUT INTERFACE	PCI SLOTS	4				
	PUERTOS SERIAL	1 PUERTO				
	PUERTOS PARALELOS	1 PUERTO				
TARJETA DE VIDEO	CANTIDAD	1				
	DESCRIPCIÓN	256MB ATI Radeon® X1300 256MB DDR SDRAM / PCI Express X16				

TARJETAS DE RED	CANTIDAD	1
	DESCRIPCIÓN	TARJETA DE RED QUAD ETHERNET PCI CONTROLLER
MEMORIA RAM	CANTIDAD	2
	CAPACIDAD	2GB DDR2 SDRAM system memory. Unbuffered, non-ECC DIMMs only

RECUPERACIÓN DEL HARDWARE		
ACCIONES PREVIAS Y DURANTE RECUPERACIÓN		
ACCIÓN	**PARAMETROS DE CONFIGURACIÓN**	**TIEMPO**
1. En Centro de Control Mazar, analizar causa del fallo de los equipos.	Revisión fisica (visual y auditiva) de errores.	20 minutos
2. Detener y Apagar equipos, en caso de no estarlo.	Desde el switch frontal de los equipos "OFF".	5 minutos
3. Desenergización de equipos.	Desconectar cables de poder de los equipos.	5 minutos
4. Retiro físico de equipos dañados.	Retirar de cúbiculos los equipos.	10 minutos
5. Copiar imagen de respaldo respectivo de cada equipo C30, CCC , CCAD en nuevos equipos.	Copia integra de imagen en nuevo disco duro de cada equipo	60 minutos
6. Instalación física de equipos nuevos	Colocar en cubículos los equipos.	10 minutos
7. Energización de equipos.	Conectar cables de poder de los equipos.	5 minutos
7. Encendido de equipos en el siguiente orden CCC, CCAD, C30	Desde el switch frontal de los equipos "ON".	30 minutos
8. Verificación de arranque de equipos	Led verde de encendido "ON"	5 minutos
VALIDACIÓN Y SINCRONIZACIÓN CON OTROS EQUIPOS		
ACCIÓN	**PARAMETROS DE CONFIGURACIÓN**	**TIEMPO**
9. Verificación de configuración de red	Visualización de conectividad entre equipos	10 minutos
PROCEDIMIENTOS PARA REGRESO AL SITIO PRINCIPAL		
ACCIÓN	**COMPLETADO SI/NO**	**TIEMPO**
N/A	N/A	N/A
N/A	N/A	N/A
OTROS PROCEDIMIENTOS POSTERIORES AL EVENTO		
ACCIÓN	**COMPLETADO SI/NO**	**TIEMPO**
INFORMACION DE PROVEEDORES DEL HARDWARE		
EMPRESA	**NOMBRE DE CONTÁCTO**	**TELÉFONO**
ALSTOM	Peter Sylva peter.sylva@power.alstom.com Luís André Marson luis.marson@power.alstom.com	**+55 (12) 3608 3544**
OBSERVACIONES		

PROCEDIMIENTO PARA RECUPERACIÓN

Identificación: Colaborador | Almacenamiento: Impreso/Digital| Archivo activo: Mientras el colaborador este activo | Retención: TIC |Vigencia: dia/mes/año | Versión: 1.0

INFORMACIÓN RELEVANTE	
CÓDIGO	PCI-PR05
NOMBRE CONTINGENCIA	Indisponibilidad PCX (principal y secundaria)
FUENTES DE RIESGO	**ESTIMACIÓN DE RIESGO**
Hardware	Alto

EQUIPO DE RECUPERACIÓN	
NOMBRE DEL EQUIPO :	Soluciones Producción Mazar SPMZ

LIDER DEL EQUIPO	
PRINCIPAL	Ing. Jaime Matute
SUPLENTE	Ing. Geovanny Dominguez / Ing. Lenin Andrade

MIEMBROS DEL EQUIPO		
	PRINCIPAL	**SUPLENTE**
1	Ing. Jaime Matute Analista de Soluciones Administrativas	Ing. Geovanny Dominguez Asistente SPMZ
2	Ing. Geovanny Dominguez Asistente SPMZ	Ing. Lenin Andrade Asistente SPMZ
3	Ing. Lenin Andrade Asistente SPMZ	

ACCIONES
1. Luego del aviso de activación del plan por parte del CPCI
2. Lider SPMZ comunica Asistente SPMZ para que realice las gestiones pertinentes con asistente de bodega y retire las PCX de repuesto para llevarlos a la planta de generación. Además de llevar el respaldo de la imagen de última configuración de las PCX.
4. Lider SPMZ y Asistente de SPMZ analizan alarmas y causas del fallo de las PCX.
5. Lider SPMZ solicita a personal de operación desenergizar las PCX.
6. Lider SPMZ y Asistente de SPMZ proceden a remplazar la PCX principal y secundaria.
7. Lider SPMZ solicita a personal de operación energizar las PCX
8. Lider SPMZ y Asistente de SPMZ verifican que las PCX esten con la última actualización y de ser necesario cargar a la PCX con el respaldo llevado en el punto 2.
9. Lider SPMZ y Analista de SPMZ realizan pruebas de funcionamiento y operatividad de las I
10. Lider SPMZ informa de la recuperación y operatividad de las PCX a Jefe de Operación y C

OBSERVACIONES
CPCI= Coordinador del Plan Contingencia Informática **SPMZ= Equipo de Soluciones de Producción Mazar** **PCX= Cell Controller** _____ **DETALLES RECUPERACIÓN HARDWARE Y SOFTWARE** **PRI-PR05.1 HARDWARE PCX** **PRI-PR05.2 SOFTWARE PCX**

PROCEDIMIENTO PARA RECUPERACIÓN

Identificación: Colaborador | Almacenamiento: Impreso/Digital| Archivo activo: Mientras el colaborador este activo | Retención: TIC |Vigencia: dia/mes/año | Versión: 1.0

INFORMACIÓN RELEVANTE	
CÓDIGO	PCI-PR05.1
NOMBRE DEL HARDWARE:	PCX U1 _U2 (principal y secundaria)
OBJETIVOS:	Documentar el procedimiento de restauración del hardware de las PCX Unidades de Generación Mazar
DISTRIBUCIÓN:	Ing. Jaime Matute Ing. Geovanny Dominguez Ing. Lenin Andrade
RTO	3 Horas 30 minutos

EQUIPO DE RECUPERACIÓN	
NOMBRE DEL EQUIPO :	Soluciones de Producción Mazar (SPMZ)

LIDER DEL EQUIPO	
PRINCIPAL	Ing. Jaime Matute
SUPLENTE	Ing. Geovanny Dominguez / Ing. Lenin Andrade

MIEMBROS DEL EQUIPO		
	PRINCIPAL	**ALTERNO**
1	Ing. Jaime Matute Analista de Soluciones Administrativas	Ing. Geovanny Dominguez Asistente SPMZ
2	Ing. Geovanny Dominguez Asistente SPMZ	Ing. Lenin Andrade Asistente SPMZ
3	Ing. Lenin Andrade Asistente SPMZ	

DETALLES DEL HARDWARE						
MARCA/MODELO	Rocky-3732EV					
PROCESADORES	Dual Socket-370 Processor support CeleronTM (P-PGA / Pentium® III 700 MHz (FC-PGA) - 133MHz FSB					
SISTEMA OPERATIVO	Windows NT (Embedded) RTX from Venturcom and the Soft Logic IEC kernel ISaGRAF PRO	**VERSIÓN**	N/A	**ACTUALIZACIÓN**	N/A	
BASE DATOS	N/A	**VERSIÓN**	N/A	**ACTUALIZACIÓN**	N/A	
FUENTE DE PODER	CANTIDAD	1				
	MODELO	ACE-920A				
	POTENCIA	200 W				
	VOLTAJE	Input: 85 to 265Vca / 47to 63 Hz Output: +5V/20A, +12V/4A, -12V/0.5A				
DISCOS DUROS	CANTIDAD	N/A				
	DESCRIPCIÓN	N/A				
	PARTICIONES	N/A				

INPUT/OUTPUT INTERFACE	PCI SLOTS	4
	PUERTOS SERIAL	2 PUERTOS RS-232 C
	PUERTOS PARALELOS	1 PUERTO
TARJETAS DE RED	CANTIDAD	1
	DESCRIPCIÓN	3COM: 1 port 100 Mbits/sec para dual link entre redundante PCX. CPU: 2 Fast Ethernet ports 100 Mbits/sec para red S8000 redundante. CARD: 2 ports para red F8000 redundante.
MEMORIA CACHE	CANTIDAD	1
	CAPACIDAD	256 Kbytes
MEMORIA RAM	CANTIDAD	1
	CAPACIDAD	256 MB SDRAM with ECC
MEMORIA COMPACT FLASH	CANTIDAD	1
	CAPACIDAD	256 MB

RECUPERACIÓN DEL HARDWARE

ACCIONES PREVIAS Y DURANTE RECUPERACIÓN

ACCIÓN	PARAMETROS DE CONFIGURACIÓN	TIEMPO
1. En Centro de Control Mazar, verificar alarmas y estado de PCX desde CCAD.	Revisión de registro de alarmas y errores.	10 minutos
2. Detener y Apagar PCX.	Acceder a CCAD 1) En el panel izquierdo -> escoger pestaña Hard, navegar por: - S8000 (S8000_S5 1) “REDE S8000” - FIELD BUS F8000_P5 (FBUS2) -UAC_U2_PCX (PCXcc) “UNIDAD GENERADORA2” 2) Clic derecho sobre el ítem seleccionado -> PCX Mintenance Server -> Primary 3) Se abre la ventana Automation cell maintenace Server 4) Iniciar sesión, opción Log-in (user: XXXX, password: XXXX) 5) Detener PCX -> option Administrative Tools -> Stop PCX… 6) Confirmar acción haciendo clic en el botón Yes 7) Restart or Shutdown the PCX ? -> Clic en Shutdown (Esperar que termine el proceso, observar los led’s) 8) Realizar el mismo proceso para la PCX Secondary 9) Luego que el proceso de detener la PCX termine,	10 minutos
3. Desenergizacion de PCX dañadas por parte de personal de operación	Abrir breakers de conexión eléctrica hacia PCX.	5 minutos
4. Retiro físico de PCX dañadas	Retirar del rack las PCX.	15 minutos
5. Instalación física de PCX nuevas	Colocar en el rack las PCX.	15 minutos
6. Energización de PCX por parte de personal de operación	Habilitar breakers de conexión eléctrica hacia PCX.	5 minutos

7. Encendido de PCX.	Desde el switch frontal de la PCX "ON".	5 minutos
8. Verificación de led de energizado PCX	Led verde de energizado encendido "ON"	5 minutos
VALIDACIÓN Y SINCRONIZACIÓN CON OTROS EQUIPOS		
ACCIÓN	**PARAMETROS DE CONFIGURACIÓN**	**TIEMPO**
10. Verificación de energizado desde CCAD	Visualización en pantalla de PCX "ON"	5 minutos
PROCEDIMIENTOS PARA REGRESO AL SITIO PRINCIPAL		
ACCIÓN	**COMPLETADO SI/NO**	**TIEMPO**
N/A	N/A	N/A
N/A	N/A	N/A
OTROS PROCEDIMIENTOS POSTERIORES AL EVENTO		
ACCIÓN	**COMPLETADO SI/NO**	**TIEMPO**
INFORMACION DE PROVEEDORES DEL HARDWARE		
EMPRESA	**NOMBRE DE CONTÁCTO**	**O**
ALSTOM	Peter Sylva peter.sylva@power.alstom.com Luis André Marson luis.marson@power.alstom.com	**+55 (12) 3608 3544**
OBSERVACIONES		

PROCEDIMIENTO PARA RECUPERACIÓN

Identificación: Colaborador | Almacenamiento: Impreso/Digital| Archivo activo: Mientras el colaborador este activo | Retención: TIC |Vigencia: dia/mes/año | Versión: 1.0

INFORMACIÓN RELEVANTE	
CÓDIGO	PCI-PR05.2
NOMBRE DEL SOFTWARE:	Imagen de Configuración y Lógicas de cargamento de PCX U1 _U2 (pricipal y secundaria).
OBJETIVOS:	Documentar el procedimiento de restauración del software de las PCX Unidades de Generación Mazar
DISTRIBUCIÓN:	Ing. Jaime Matute Ing. Geovanny Dominguez Ing. Lenin Andrade
RTO	3 Horas 30 minutos

EQUIPO DE RECUPERACIÓN	
NOMBRE DEL EQUIPO :	Soluciones de Producción Mazar (SPMZ).

LIDER DEL EQUIPO	
PRINCIPAL	Ing. Jaime Matute /Ing. Lenin Andrade
SUPLENTE	Ing. Geovanny Dominguez / Ing. Lenin Andrade

MIEMBROS DEL EQUIPO		
	PRINCIPAL	**ALTERNO**
1	Ing. Jaime Matute Analista de Soluciones Administrativas	Ing. Geovanny Dominguez Asistente SPMZ
2	Ing. Geovanny Dominguez Asistente SPMZ	Ing. Lenin Andrade Asistente SPMZ
3	Ing. Lenin Andrade Asistente SPMZ	

DETALLES DEL SOFWARE	
1	Imágen de configuración de arranque de PCX
2	Lógicas y Controladores de PCX

SISTEMA OPERATIV	N/A	**VERSIÓN**	N/A	**ACTUALIZACIÓN**	N/A
BASE DATOS	N/A	**VERSIÓN**	N/A	**ACTUALIZACIÓN**	N/A

RECUPERACIÓN DEL SOFTWARE

ACCIONES PREVIAS Y DURANTE RECUPERACIÓN

ACCIÓN	PARÁMETROS DE CONFIGURACIÓN	TIEMPO
1.Verificar desde CCAD que imágen de configuracion de respaldo que se encuentra en memoria flash, es la última.	Se verifica fecha de respaldo con últimas configuración guaradda en CCAD.	5minutos
2. Si se verifica que no es el último respaldo de la imágen de configuración, realizar una copia de la última imagen desde CCAD hacia memoria flash de PCX.	En CCAD Navegar por: - S8000 (S8000_S5 1) “REDE S8000” - FIELD BUS F8000_P5 (FBUS2) “” - UAC_U1_PCX (PCXcc) “UNIDAD GENERADORA1” ó UAC_U2_PCX (PCXcc) “UNIDAD GENERADORA2” - Clic derecho sobre el ítem seleccionado -> Generate Code -> Generate With Automatic Code	10minutos

3. Verificación de led de energizado PC	Led verde de energizado encendido "ON"	5 minutos
4. Conectar monitor y teclado a la PCX para poder ver todo el proceso de arranque de la PCX.	Monitor y teclado conectados a los puertos correspondientes de la PCX.	10minutos
5. Insertar memoria flash (configuración) en PCX.	Memoria Flash 256MB.	2minutos
6. Encender PCX y configurar la BIOS.	Encender switch frontal de PCX "ON" Navegar por AwardBIOS CMOS Setup Utility (Ver archivo de configuración de la BIOS)	10 minutos
7. La PCX se reinicia automáticamente al terminar de configurar la BIOS.	Proceso automatico de reinicio.	5 minutos
8. Verificar leds de estado de PCX.	Led RUN "ON" Servicios encendidos, "OFF" servicios apagados Led Defalts apagado "OFF" Led Master/Slave "ON" si se le asigna rol de PCX master , "OFF" si esta en Stanby Led Primary / Secondary "ON" si se le asigna rol de PCX primary, "OFF" si es secondary .	5 minutos
9. Conetar la CCAD cliente a la red Office y levantar el aplicativo de Administración de CCAD.	Utilizar cable de red LAN RJ45	2 minutos
10. Realizar el cargamento de lógicas y controladores de las PCX desde CCAD cliente.	-Desde CCAD confirmar acción detener de todos los controladores asociados a la PCX -Si algún controlador aún no se detiene, detenerlo de forma individual. -Clic en el botón Store Operation (a continuación del botón Stop Cell) -Esperar por el proceso Store UAC2_U2_PCX in progress…	60 minutos
11. La PCX se detiene automaticamente para cargamento, una vez cargado todos los controladores, iniciarlos (Run) nuevamente.	Desde PCX Http Server, reiniciar PCX Firmware. Log-in -> menú Administrative Tools -> PCX Firmware Update -> Current Release -> botón Restart.	2 minutos
12. Revisar registros (logs) en el cento de control Mazar desde CIS ó CCC ó CCAD e ingresar a PCX a confirmar que todo este funcionando OK. Si no esta Ok, volver al punto 6.	Revisión de funcionamiento	10 minutos
13. Revisar alarmas en el SCADA (Todo operativo, control, consignas configuraciones y datos correctos). Si no esta Ok, volver al punto 6.	Revisión de funcionamiento	20 minutos
14. Desconectar monitor y teclado de la PCX conectados previamente.	Retiro de equipos de configuración	10 minutos
VALIDACIÓN Y SINCRONIZACIÓN CON OTROS EQUIPOS		
ACCIÓN	**PARAMETROS DE CONFIGURACIÓN**	**TIEMPO**
PROCEDIMIENTOS PARA REGRESO AL SITIO PRINCIPAL		

ACCIÓN	COMPLETADO SI/NO	TIEMPO
OTROS PROCEDIMIENTOS POSTERIORES AL EVENTO		
ACCIÓN	**COMPLETADO SI/NO**	**TIEMPO**
INFORMACION DE PROVEEDORES DEL SOFTWARE		
EMPRESA	**NOMBRE / EMAIL DE CONTÁCTO**	**TELÉFONO**
ALSTOM	Peter Sylva peter.sylva@power.alstom.com Luís André Marson luis.marson@power.alstom.com	+55 (12) 3608 3544
OBSERVACIONES		

PROCEDIMIENTO PARA RECUPERACIÓN

Identificación: Colaborador | Almacenamiento: Impreso/Digital| Archivo activo: Mientras el colaborador este activo | Retención: TIC |Vigencia: dia/mes/año | Versión: 1.0

INFORMACIÓN RELEVANTE	
CODIGO	PCI-PR06
NOMBRE CONTINGENCIA	Indisponibilidad Red S8000
FUENTES DE RIESGO	**ESTIMACIÓN DE RIESGO**
Hardware	Alto

EQUIPO DE RECUPERACIÓN	
NOMBRE DEL EQUIPO :	Redes y Comunicaciones RCMZ

LIDER DEL EQUIPO	
PRINCIPAL	Ing. Santiago Alvarez
SUPLENTE	Ing. Diego Tello / Ing. Andres Alvarez

MIEMBROS DEL EQUIPO		
	PRINCIPAL	**SUPLENTE**
1	Ing. Santiago Alvarez Analista de Redes y Comunicaciones	Ing. Diego Tello Asistente RCMZ
2	Ing. Diego Tello Asistente RCMZ	Ing. Andres Alvarez Asistente RCMZ
3	Ing. Andres Alvarez Asistente RCMZ	

ACCIONES
1. Luego del aviso de activación del plan por parte del CPCI
2. Lider RCMZ comunica Asistente RCMZ para que realice las gestiones pertinentes con asistente de bodega y retire los Switchs de repuesto para llevarlos a la planta de generación.
3. Lider RCMZ y Asistente de RCMZ analizan causa del fallo de la red.
4. Lider RCMZ y Asistente de RCMZ desenergizan los equipos.
5. Lider RCMZ y Asistente de RCMZ proceden a remplazar los equipos.
6. Lider SPMZ y Asistente de SPMZ energizan los equipos.
7. Lider SPMZ y Analista de SPMZ realizan pruebas de funcionamiento y operatividad de los e
8. Lider RCMZ informa de la recuperación y operatividad de la red a Jefe de Operación y CPCI

OBSERVACIONES
CPCI= Coordinador del Plan Contingencia Informática **RCMZ= Equipo de Redes y Comunicación Mazar** **S8000= Red tipo ring de sistema SCADA para conectividad C30 CCG CCAD y PCX** **Switchs= Equipos de comunicación de red S8000**

PROCEDIMIENTO PARA RECUPERACIÓN

Identificación: Colaborador | Almacenamiento: Impreso/Digital| Archivo activo: Mientras el colaborador este activo | Retención: TIC |Vigencia: dia/mes/año | Versión: 1.0

INFORMACIÓN RELEVANTE	
CÓDIGO	PCI-PR07
NOMBRE CONTINGENCIA	Indisponibilidad Red F8000
FUENTES DE RIESGO	**ESTIMACIÓN DE RIESGO**
Hardware	Alto

EQUIPO DE RECUPERACIÓN	
NOMBRE DEL EQUIPO :	Redes y Comunicaciones RCMZ

LIDER DEL EQUIPO	
PRINCIPAL	Ing. Santiago Alvarez
SUPLENTE	Ing. Diego Tello / Ing. Andres Alvarez

MIEMBROS DEL EQUIPO		
	PRINCIPAL	**SUPLENTE**
1	Ing. Santiago Alvarez Analista de Redes y Comunicaciones	Ing. Diego Tello Asistente RCMZ
2	Ing. Diego Tello Asistente RCMZ	Ing. Andres Alvarez Asistente RCMZ
3	Ing. Andres Alvarez Asistente RCMZ	

ACCIONES
1. Luego del aviso de activación del plan por parte del CPCI
2. Lider RCMZ comunica Asistente RCMZ para que realice las gestiones pertinentes con asistente de bodega y retire los Switchs de repuesto para llevarlos a la planta de generación.
3. Lider RCMZ y Asistente de RCMZ analizan causa del fallo de la red.
4. Lider RCMZ y Asistente de RCMZ desenergizan los equipos.
5. Lider RCMZ y Asistente de RCMZ proceden a remplazar los equipos.
6. Lider SPMZ y Asistente de SPMZ energizan los equipos.
7. Lider SPMZ y Analista de SPMZ realizan pruebas de funcionamiento y operatividad de los e
8. Lider RCMZ informa de la recuperación y operatividad de la red a Jefe de Operación y CPCI

OBSERVACIONES
CPCI= Coordinador del Plan Contingencia Informática **RCMZ= Equipo de Redes y Comunicación Mazar** **F8000= Red tipo ring de sistema SCADA para Fields Control** **Switchs= Equipos de comunicación de red F8000**

ANEXO F

EQUIPO DEL PLAN DE CONTINGENCIA INFORMÁTICO

Identificación: Colaborador | Almacenamiento: Impreso/Digital| Archivo activo: Mientras el colaborador este activo | Retención: TIC |Vigencia: dia/mes/año | Versión: 1.0

INFORMACIÓN RELEVANTE	
CÓDIGO	PCI-PR08

COORDINADOR DEL PLAN

NOMBRE DEL FUNCIONARIO	ROL	TELÉFONO	CELULAR	DIRECCIÓN
Ing. Marcelo Monteros	Coordinador			

MIEMBROS DEL EQUIPO

EQUIPO	NOMBRE DEL FUNCIONARIO	ROL	TELÉFONO	CELULAR	DIRECCIÓN
RCMZ	Ing. Santiago Alvarez	LIDER RCMZ			
	Ing. Diego Tello	EJECUTOR RCMZ			
	Ing. Andres Alvarez	EJECUTOR RCMZ			
SPMZ	Ing. Jaime Matute	LIDER SPMZ			
	Ing. Geovanny Dominguez	EJECUTOR SPMZ			
	Ing. Lenin Andrade	EJECUTOR SPMZ			
OPMZ	Ing. Armando Bernal	LIDER OPMZ			
	Operador de Turno Sala de Control	EJECUTOR OPMZ			
	Operador de Turno Sala de Control	EJECUTOR OPMZ			

ANEXO G

CONTÁCTOS EXTERNOS

Identificación: Colaborador | Almacenamiento: Impreso/Digital| Archivo activo: Mientras el colaborador este activo | Retención: TIC |Vigencia: dia/mes/año | Versión: 1.0

INFORMACIÓN RELEVANTE			
CÓDIGO	PCI-PR09		
EMPRESA	ALSTOM		
SERVICIO	HARDWARE Y SOFTWARE		
TELÉFONO	+55 (12) 3608 3544		
DIRECCIÓN	Sao Paulo Brasil Avenida Charles Schneider s/n, Pq. Senhor do Bonfim, Taubaté-SP, CEP 12040-001		
EMAIL	N/A		
RELACIÓN CON ACTIVO CRÍTICO	ALSPA 320		
NOMBRE DEL CONTÁCTO	**EMAIL**	**TELÉFONO**	**CELULAR**
Peter Sylva	peter.sylva@power.alstom.com	+55 (12) 3608 3544	
Luis André Marson	luis.marson@power.alstom.com	+55 (12) 3608 3544	

ANEXO H

ESTADO DEL ACTIVO INFORMÁTICO

Identificación: Colaborador | Almacenamiento: Impreso/Digital| Archivo activo: Mientras el colaborador este activo | Retención: TIC |Vigencia: dia/mes/año | Versión: 1.0

CÓDIGO	PCI-PR09		
TIPO DE INCIDENTE		**LUGAR DEL INCIDENTE :**	
NOMBRE DE QUIÉN LLENA REPORTE :			

ESTADO	*CONDICIÓN	TIEMPO RECUPERACIÓ	COMENTARIOS

*CONDICIÓN
ND -> No dañado
DPU-> Dañado pero utilizable
DR-> Dañado requiere reparación antes de usar
D-> Dañado

FIRMA

ANEXO I

EVALUAR RESULTADOS

Identificación: Colaborador | Almacenamiento: Impreso/Digital| Archivo activo: Mientras el colaborador este activo | Retención: TIC |Vigencia: dia/mes/año | Versión: 1.0

CÓDIGO	PCI-PR10		
TIPO DE INCIDENTE		**LUGAR DEL INCIDENTE :**	
NOMBRE DE QUIÉN LLENA REPORTE :			

DESCRIPCIÓN DE ACCIONES	FUNCIONO SI/NO	PORQUÉ Y COMO MEJORAR

FIRMA

ANEXO J

CALENDARIO DE PRUEBAS

Identificación: Colaborador | Almacenamiento: Impreso/Digital| Archivo activo: Mientras el colaborador este activo | Retención: TIC |Vigencia: dia/mes/año | Versión: 1.0

INFORMACIÓN RELEVANTE			
CÓDIGO	PCI-PR11		
ELABORADO POR:		**ROL EN EL PLAN:**	
AÑO			

TIPO	DESCRIPCIÓN	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	OBSERVACIONES

FIRMA

BIBLIOGRAFÍA

[1] Soler de Arespacochaga, J., La Seguridad Informática: Planes de Contingencia,http://www.mapfre.com/documentacion/publico/i18n/catalogo_imagenes/grupo.cmd?path=1009130, fecha de consulta agosto 2014, páginas 19-32

[2] Borghello, C., Plan de Contingencia, http://www.segu-info.com.ar/politicas/contingencia.htm , fecha de consulta agosto 2014

[3] Teckelino, T., Plan de contingencia sistemas informáticos, http://es.scribd.com/doc/43714047/Plan-de-contingencia-sistemas-informaticos#scribd , fecha de consulta septiembre 2014

[4] Vieites, A., Enciclopedia de la Seguridad Informática, Ra-Ma 2.a Edición, 2011

[5] NIST, National Institute of Standards and Technology., Contingency Planning Guide for Federal Information Systems, http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf , fecha de consulta octubre 2014

[6] Ministerio de Hacienda y Administraciones Públicas España, Magerit Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información,http://administracionelectronica.gob.es/pae_Home/pae_Doc

umentacion/pae_Metodolog/pae_Magerit.html#.VXbjv8-qpHw , fecha de consulta octubre 2014

[7] Quintero, J., Análisis y Gestión de Riesgos Herramienta PILAR, http://www.aec.es/c/document_library/get_file?p_l_id=64199&folderId=1081319&name=DLFE-11743.pdf , fecha de consulta diciembre 2014

[8] CELEC EP., Reseña Histórica, https://www.celec.gob.ec/quienes-somos/resena-historica.html , fecha de consulta diciembre 2014

[9] Ministerio de Electricidad y Energía Renovable, Concepto de Energía renovable, http://www.energia.gob.ec/subsecretaria-de-energia-renovable-y-eficiencia-energetica/ , fecha de consulta diciembre 2014

[10] Flores, S., Sistema de Gestión de Continuidad de Negocios, ISEC-Information Security Inc., 2014

[11] CELEC EP Hidropaute., Filosofía Corporativa. https://www.celec.gob.ec/hidropaute/perfil-corporativo/filosofia-corporativa.html , fecha de consulta diciembre 2014

[12] Seguro Social Costa Rica, Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones,http://www.academia.edu/9225021/Caja_Co

starricense_de_Seguro_Social_Tabla_de_Contenidos , fecha de consulta febrero 2015

[13] INTECO, Guía práctica para PYMES: cómo implantar un Plan de Continuidad de Negocio, https://www.incibe.es/CERT/guias_estudios/guias/guia_continuidad , fecha de consulta febrero 2015